Signamax Connectivity Systems
Model 065-7941
24-Port 10/100/1000BaseT/TX
WebSmart Switch
U s e r’s G u i d e

Signamax Connectivity Systems
Model 065-7941

24-Port 10/100/1000BaseT/TX
WebSmart Switch
U s e r's G u i d e

Release 1.0

Release Date: July, 2005

Signamax Connectivity Systems
1810 N.E 144th Street
N. Miami, FL 33181
800-446-3277
www.Signamax.com

Table of Contents

CAUTION ---------- VI
ELECTRONIC EMISSION NOTICES ---------- VI

CHAPTER 1. INTRODUCTION ---------- 2

1-1. OVERVIEW OF THE 065-7941 WEBSMART SWITCH ---------- 2
1-2. CHECKLIST ---------- 3
1-3. FEATURES ---------- 3
1-4. VIEW OF THE 065-7941 WEBSMART SWITCH ---------- 5
1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs) ----- 5
1-4-2. User Interfaces on the Rear Panel ---------- 6
1-5. VIEW OF THE OPTIONAL MODULES ---------- 7

CHAPTER 2. INSTALLATION ---------- 8

2-1. STARTING UP THE 065-7941 WEBSMART SWITCH ---------- 8
2-1-1. Hardware and Cable Installation ---------- 8
2-1-2. Cabling Requirements ---------- 9
2-1-2-1. Cabling Requirements for TP Ports ---------- 10
2-1-2-2. Cabling Requirements for 1000SX/LX SFP Module ---------- 10
2-1-2-3. Switch Cascading in Network Topology ---------- 11
2-1-3. Configuring the Management Agent of the 065-7941 WebSmart switch ---------- 14
2-1-3-1. Configuring the Management Agent of the 065-7941 WebSmart switch through the Ethernet Port ---------- 15
2-1-4. IP Address Assignment ---------- 16
2-2. TYPICAL APPLICATIONS ---------- 21

CHAPTER 3. BASIC CONCEPT AND MANAGEMENT ---------- 23

3-1. WHAT'S ETHERNET? ---------- 23
3-2. MEDIA ACCESS CONTROL (MAC) ---------- 26
3-3. FLOW CONTROL ---------- 32
3-4. HOW DOES A SWITCH WORK? ---------- 35
3-5. VIRTUAL LAN ---------- 39
3-6. LINK AGGREGATION ---------- 45

CHAPTER 4. OPERATION OF WEB-BASED MANAGEMENT ---------- 47

4-1. WEB MANAGEMENT HOME OVERVIEW ---------- 48
4-2. CONFIGURATION ---------- 50
4-2-1. System Configuration ---------- 51
4-2-2. Ports Configuration ---------- 54
4-2-3. VLAN Mode Configuration ---------- 56

4-2-4. VLAN Group Configuration----------59
4-2-5. PVID Configuration----------62
4-2-6. Aggregation Configuration----------64
4-2-7. Mirror Configuration----------65
4-2-8. Quality of Service Configuration ----------66
4-2-9. Bandwidth Management ----------75
4-2-10. Trap Event Configuration----------77
4-2-11. Max. Packet Length ----------78
4-3. MONITORING ----------79
4-3-1. Statistics Overview ----------79
4-3-2. Detailed Statistics----------80
4-4. MAINTENANCE ----------83
4-4-1. Status----------83
4-4-1-1.System Status ----------84
4-4-1-2. TP / Fiber Ports Status----------86
4-4-1-3. Aggregation----------88
4-4-1-4. VLAN----------89
4-4-1-5. Mirror----------91
4-4-1-6. Trap Event ----------92
4-4-1-7. Maximum Packet Length----------93
4-4-2. Warm Restart----------94
4-4-3. Factory Default----------95
4-4-4. Logout ----------96

CHAPTER 5. MAINTENANCE----------97

5-1. RESOLVING A NO LINK CONDITION----------97
5-2. Q&A----------97

APPENDIX A TECHNICAL SPECIFICATIONS ----------98

Revision History

Release	Date	Revision
1.0	8/17/2005	A1

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

About this user's manual

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the 065-7941 Switch through the built-in Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown, as well as examples of the operation of the web-based user interface (UI).

Overview of this user's manual

- Chapter 1 "Introduction" describes the features of the 065-7941 Gigabit WebSmart Switch
- Chapter 2 "Installation"
- Chapter 3 "Operating Concept and Management"
- Chapter 4 "Operation of Web-based Management"
- Chapter 5 "Maintenance"

1. Introduction

1-1. Overview of the 065-7941 24-Port Gigabit WebSmart Switch

The 065-7941 24-port Gigabit WebSmart Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet, and Standard Ethernet specifications. The switch includes 22 10/100/1000 Mbps Twisted Pair (TP) ports and 2 Gigabit dual media TP/SFP (Small Form-factor Pluggable) fiber ports. The switch can be managed through any Ethernet port using a Web-based management user interface: with web-based management, the network administrator can log on to the switch to monitor, configure and control each port's activity. In addition, the switch implements QoS (Quality of Service), VLAN, and Trunking. It is suitable for virtually any office application.

In this switch, Port 23, 24 includes two types of media --- TP and SFP Fiber (LC, BiDi-LC…); this port supports 10/100/1000 Mbps TP or 1000 Mbps SFP Fiber with auto-detected function. 1000 Mbps SFP Fiber transceiver is used for high-speed connection expansion.

- 1000 Mbps LC, Multi-Mode, SFP Fiber transceiver
- 1000 Mbps LC, 10 Km, SFP Fiber transceiver
- 1000 Mbps LC, 30 Km, SFP Fiber transceiver
- 1000 Mbps LC, 50 Km, SFP Fiber transceiver
- 1000 Mbps BiDi-LC, 20 Km, 1550 nm SFP Fiber WDM transceiver
- 1000 Mbps BiDi-LC, 20 Km, 1310 nm SFP Fiber WDM transceiver

10/100/1000 Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. 1000 Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000 Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

• Key Features in the Device

QoS:

The switch offers powerful QoS function. This function supports TOS field of IP header (equal DSCP low 3 bits) on Layer 3 of network framework and 6 kinds of special network transmission events on Layer 4.

VLAN:

Supports Port-based VLAN, IEEE 802.1Q Tag VLAN. And supports 24 active VLANs and VLAN ID 1~4094.

Port Trunking:

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- The 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch
- Mounting Accessory (for 19” Rack Shelf)
- This User's Manual in CD-ROM format
- AC Power Cord

Please notify your sales representative immediately if any of the aforementioned items are missing or damaged.

1-3. Features

The 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

• Hardware

- 22 10/100/1000 Mbps Auto-negotiation Gigabit Ethernet TP ports
- 2 10/100/1000 Mbps TP or 1000 Mbps SFP Fiber dual media auto sense
- 400 KB on-chip frame buffer
- Jumbo frame support
- Programmable ingress classifier for QoS (Layer 4/Multimedia)
- 8K MAC address and 4K VLAN support (IEEE 802.1Q)
- Per-port shaping, policing, and Broadcast Storm Control
- IEEE 802.1Q-in-Q nested VLAN support
- Full-duplex flow control (IEEE 802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, TP Ports 1-24: LINK/ACT, 10/100/1000 Mbps, SFP Port 23 & 24: SFP (LINK/ACT)

• Management

- Supports port status display and easy port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system Information when you login
- Supports the port mirroring function
- Supports the static trunk function

- Supports 802.1Q VLAN
- Supports user management and limits login to one user
- Maximum packet length can be up to 9216 bytes for jumbo frame applications
- Supports Broadcasting Suppression to avoid network suspension or crash
- Supports sending trap events while monitored events happen
- Supports a default configuration which can be restored to overwrite the current configuration on which the switch is working via the Web UI and the switch's Reset button
- Supports on-line plug/unplug of SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- Built-in web-based management instead of using CLI interface, providing a more convenient Graphical User Interface for the user

1-4. View of the 065-7941 24-Port Gigabit WebSmart Switch

Fig. 1-1 Full View of the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch

1-4-1. User Interfaces on the Front Panel (Buttons, LEDs and Plugs)

There are 24 TP Gigabit Ethernet ports and 2 SFP fiber ports for optional removable modules on the front panel of the switch. The LED display area, located on the left side of the panel, contains a Power LED, which indicates the power status and the working status of the 24 ports on the switch.

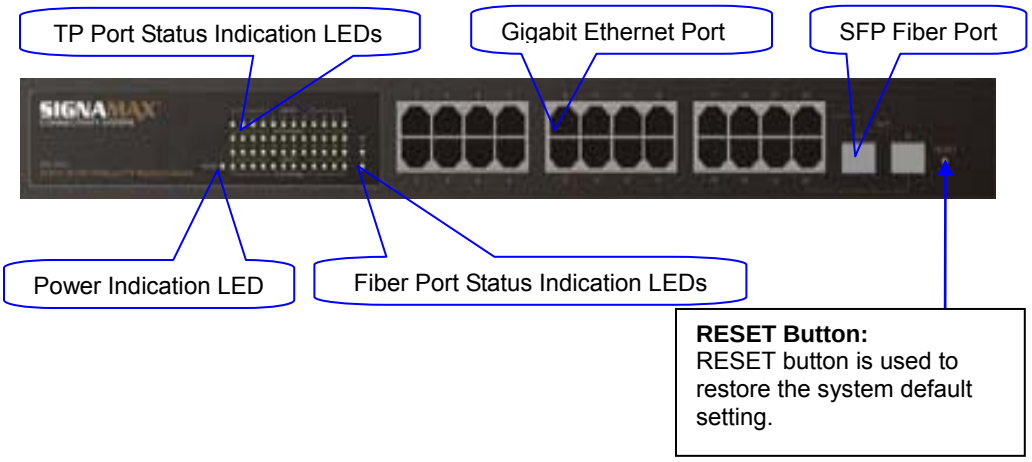

TP Port Status Indication LEDs
Gigabit Ethernet Port
SFP Fiber Port
Power Indication LED
Fiber Port Status Indication LEDs
RESET Button:
RESET button is used to restore the system default setting.

Fig. 1-2 Front View of the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch

• LED Indicators

LED	Color	Function
System LED		
POWER	Green	Lit when +5 V DC power is on and good
10/100/1000Ethernet TP Port 1 to 24 LED		
LINK/ACT	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when cable connection is not good
10/100/1000 Mbps	Green/ Amber	Lit green when 1000 Mbps speed is active Lit amber when 100 Mbps speed is active Off when 10 Mbps speed is active
1000SX/LX Gigabit Fiber Port 23, 24 LED		
SFP (LINK/ACT)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Table1-1

1-4-2. User Interfaces on the Rear Panel

Fig. 1-3 Rear View of the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch

1-5. View of the Optional Modules

In this switch, both Ports 23 & 24 include two types of media --- TP and SFP Fiber (LC, BiDi LC).This port supports either 10/100/1000 Mbps TP or 1000 Mbps SFP Fiber with an auto-detection function. The 1000 Mbps SFP Fiber transceiver is used for high-speed connection expansion; nine optional SFP types provided for the switch are listed below:

- 1000 Mbps LC, MM, SFP Fiber transceiver
- 1000 Mbps LC, SM 10 Km, SFP Fiber transceiver
- 1000 Mbps LC, SM 30 Km, SFP Fiber transceiver
- 1000 Mbps LC, SM 50 Km, SFP Fiber transceiver
- 1000 Mbps BiDi LC, type 1, SM 20 Km, SFP Fiber WDM transceiver
- 1000 Mbps BiDi LC, type 2, SM 20 Km, SFP Fiber WDM transceiver
- 1000 Mbps LC, SM 10 Km, SFP Fiber transceiver with DDM

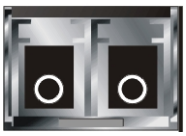


Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

Fig. 1-5 Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

2. Installation

2-1. Starting Up the 065-7941 24-Port Gigabit WebSmart Switch

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

Before beginning the installation, please do the following:

⇒ Wear a grounding device to avoid the damage from electrostatic discharge

⇒ Be sure that the power switch is OFF before you insert the power cord to the power source

• Installing Optional SFP Fiber Transceivers to the 065-7941 Gigabit WebSmart Switch

Note: If you have no modules, please skip this section.

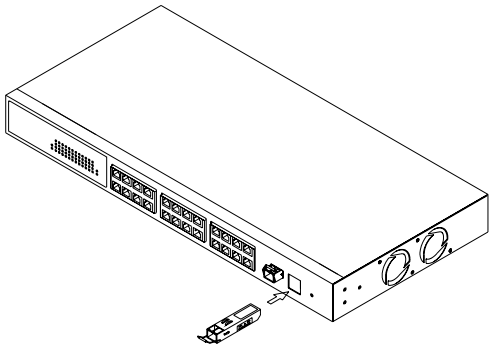


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

• Connecting the SFP Module to the Chassis:

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into the slot(s)
5. Turn the power ON after the above procedures are done, if the switch was not powered on

- **TP Port and Cable Installation**

⇒ In this switch, each TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100 M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossover (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. Either type can be used successfully, and can be mixed on different switch ports.

⇒ Use Cat. 5e or better grade RJ-45 TP cable to connect to a TP port of the switch, and the other end of the cable is then connected to a network-aware device such as a workstation or a server.

⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

The switch is now ready to operate..

• Power On

The switch supports power sourced from a 100-240 V AC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection is plugged into the switch or not when power on, even the SFP modules as well. After the power is on, all LED indicators will light up immediately and then all will turn off except the power LED, which remains on. This represents a reset of the system.

• Firmware Loading

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds; after that, the switch will flash all the LEDs once and automatically performs a self-test and is then in a ready state.

2-1-2. Cabling Requirements

To help ensure a successful installation and keep the network performance as high as possible, please observe the cabling requirements. Cables with a lower specification will cause the LAN not to perform as specified.

2-1-2-1. Cabling Requirements for TP Ports

⇒ For Fast Ethernet TP network connection
— The grade of the cable must be Cat. 5 or better, with a maximum length of 100 meters.
⇒ Gigabit Ethernet TP network connection
— The grade of the cable must be Cat. 5e or better, with a maximum length of 100 meters. Cat. 6 is recommended.

2-1-2-2. Cabling Requirements for 1000SX/LX SFP Module

Fiber optic media is more complex and comprehensive compared to TP cabling. There are two categories of fiber, multimode (MM) and singlemode (SM). The various Gigabit singlemode fiber specification types are categorized into several classes by the distances they support. These categories are 1000BaseSX, 1000BaseLX, 1000BaseLH, 1000BaseXD, and 1000BaseZX. From the viewpoint of connector type, the main types used in SFP modules are LC and BIDI LC.

— Gigabit Fiber with multi-mode LC SFP module
— Gigabit Fiber with single-mode LC SFP module
— Gigabit Fiber with BiDi LC 1310 nm SFP module
— Gigabit Fiber with BiDi LC 1550 nm SFP module

The following table lists the types of fiber that Signamax supports; those not listed here are available upon request.

<table>
<tr><td rowspan="4">IEEE 802.3z Gigabit Ethernet 1000SX 850 nm</td><td colspan="4">Multi-mode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125μm</td><td colspan="2">Multi-mode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160 MHz-Km</td><td>220 m</td><td>400 MHz-Km</td><td>500 m</td></tr>
<tr><td>200 MHz-Km</td><td>275 m</td><td>500 MHz-Km</td><td>550 m</td></tr>
<tr><td rowspan="3">1000Base-LX/LHX/XD/ZX</td><td colspan="4">Single-mode Fiber 9/125 μm</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310 nm 10 Km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550 nm 30, 50 Km</td></tr>
<tr><td rowspan="4">1000Base-LX Single Fiber (BIDI SC)</td><td colspan="2" rowspan="2">Single-Mode *20 Km</td><td>TX(Transmit)</td><td>1310 nm</td></tr>
<tr><td>RX(Receive)</td><td>1550 nm</td></tr>
<tr><td colspan="2" rowspan="2">Single-Mode *20 Km</td><td>TX(Transmit)</td><td>1550 nm</td></tr>
<tr><td>RX(Receive)</td><td>1310 nm</td></tr>
</table>

Table2-1

2-1-2-3. Switch Cascading in Network Topology

• Takes the Delay Time into Account

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may uplink the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraints of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Converter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01μs (1 sec./100 Mega bit)			

Table 2-2

The sum of all elements' bit-time delay and the overall bit-time delay of the wires/devices must be within the Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this limitation is not applicable. You may use the SFP module or full-duplex media converters connected to the TP ports of the switch to extend the TP node distance over fiber optic cabling and provide the long haul connection.

• Typical Network Topology in Deployment

A hierarchical network with minimum levels of switching may reduce the timing delay between server and client station. Using this approach, the number of switches in any one path is minimized; this will reduce the possibility of network loops and will improve network efficiency. If more than two switches are connected in the same network, select one switch as the Level 1 switch and connect all other switches to it at Level 2. Servers and/or Hosts are recommended to be connected to the Level 1 switch. These general recommendations should be followed if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-2).

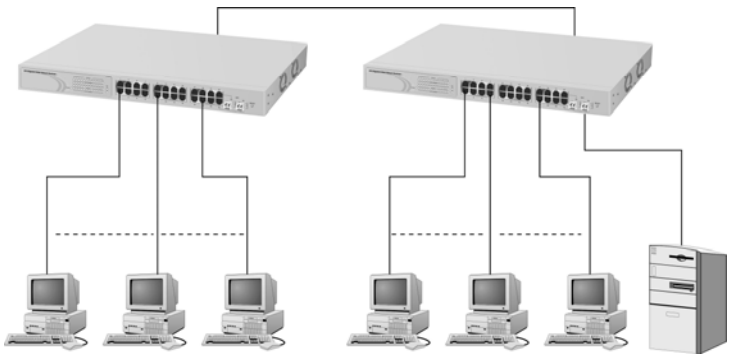


Fig. 2-2 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate with each other directly is bounded in the same VLAN area.

Here, the VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the differences are.

Case2a: Port-based VLAN (See Fig.2-3).

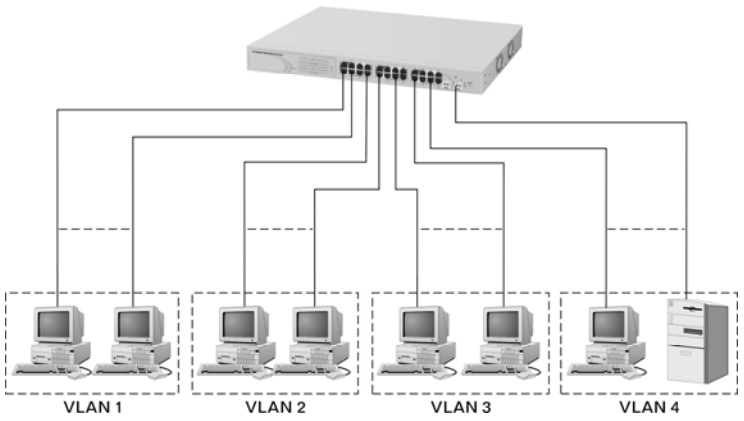


Fig. 2-3 Port-based VLAN Diagram

1. The same VLAN members cannot be in different switches.
2. Each VLAN's members cannot access members of another VLAN.
3. The administrator has to assign different names for each of the VLAN groups in one switch.

Case 2b: Port-based VLAN (See Fig.2-4).

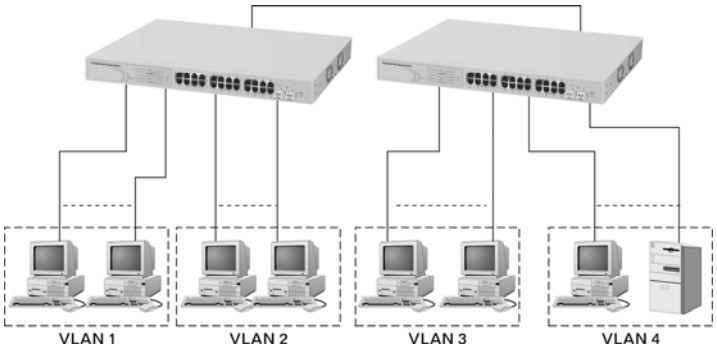


Fig. 2-4 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-5).

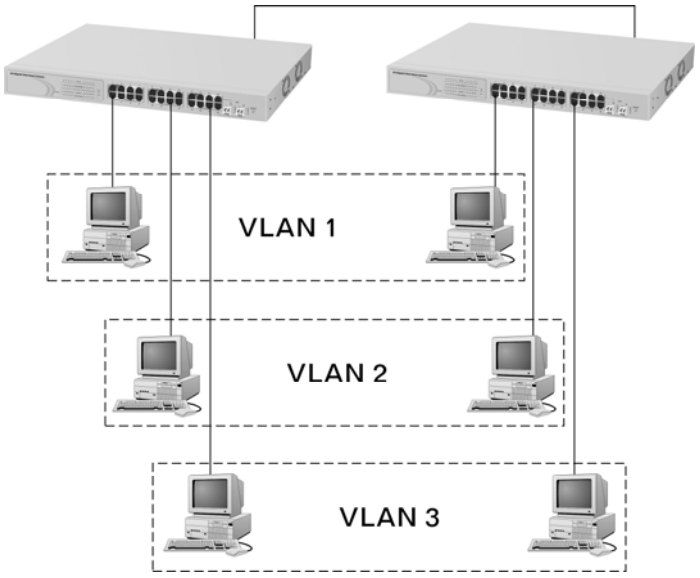


Fig. 2-5 Attribute-based VLAN Diagram

2-1-3. Configuring the Management Agent of the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch

Through the use of a web browser, the user is allowed to begin the switch management function. The user can use any one of the ports to monitor and configure the switch. You can manage and administer the switch through the following procedures.

Section 2-1-3-1: Configuring the Management Agent of the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch through an Ethernet Port

2-1-3-1. Configuring Management Agent of the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch through an Ethernet Port

There are two ways to configure and monitor the switch through the switch's Ethernet port: by using a Web browser and by using an SNMP manager. The user interface for the SNMP manager is NMS dependent and is not covered here; the Web-based UI for the switch is a highly user-friendly interface.

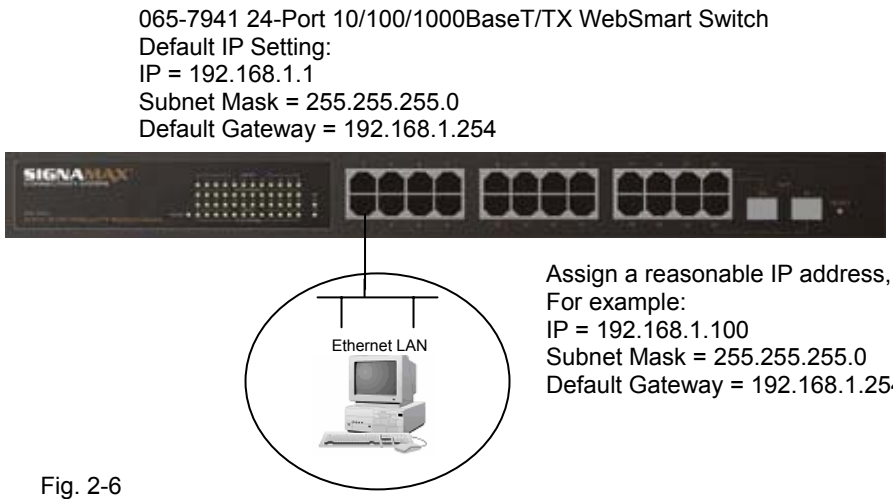


Fig. 2-6

• Managing the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch through an Ethernet Port

Before the user communicates with the switch, they must first finish the configuration of the IP address or know the current IP address of the switch. Then, the user must follow the procedures listed below.

1. Set up a physical path between the configured the switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

   Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. However, the subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-6 regarding the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch default IP address information.

2. Run the web browser and follow the menu. Please refer to Chapter 4.

Fig. 2-7 the Login Screen for Web UI

2-1-4. IP Address Assignment

For IP address configuration, there are three parameters that need to be filled in. They are the IP address, Subnet Mask, and the Default Gateway.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks as shown in Fig. 2-8. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bit address. Each IP address is comprised of two parts: the network identifier (address) and the host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of the host refers to. The host identifier must also be unique in the same LAN. The version of the IP address used in this switch is version 4, known as IPv4.

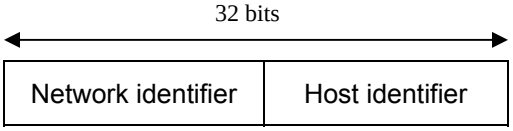
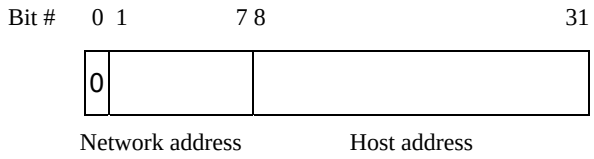


Fig. 2-8 IP address structure

Classful addressing divides IP address into three classes: class A, class B and class C. The remaining valid IP addresses are used for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

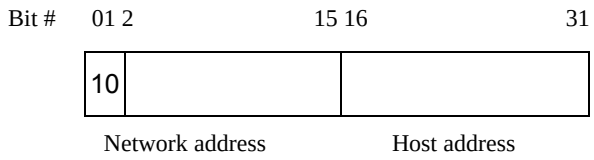
Class A:

Valid addresses are those less than 126.255.255.255. There are a total of 126 networks that can be defined, because address 0.0.0.0 is reserved for the default route and 127.0.0.0/8 is reserved for the loopback function.



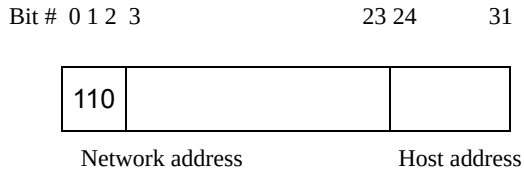
Class B:

Valid IP addresses range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed by a 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined, with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

Valid IP addresses range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed by an 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 – 2) hosts per network.



Class D and E:

Class D is a class with the first 4 MSB (Most Significant Bits) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with the first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it a Private IP address, and list them below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

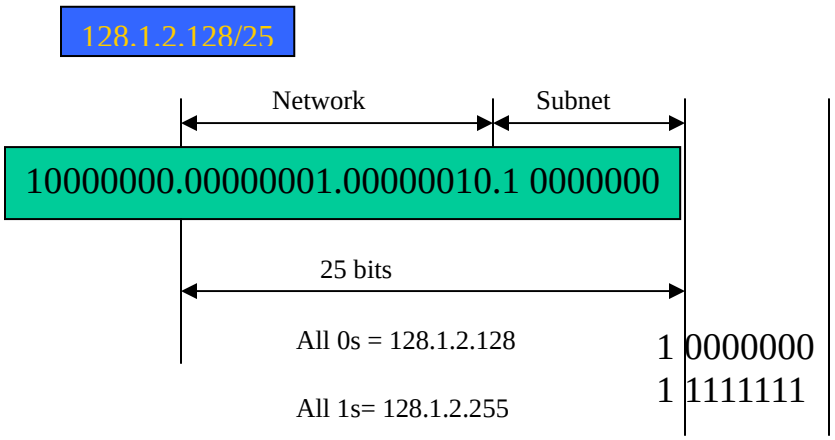
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

Subnet mask means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address on a bitwise basis. It is designed to utilize IP addresses more efficiently and ease the management of an IP network.

For a class B network, using the example 128.1.2.3, that network may have a subnet mask 255.255.0.0 as the default, in which the first two bytes will be all 1s. This means more than 60 thousand nodes in flat IP addresses will be at the same network. Such a network is too large to practically manage. If the network is divided into a smaller network by extending its network prefix from 16 bits to, say 24 bits, that uses its third byte to subnet this class B network. That network now has a subnet mask of 255.255.255.0, in which each bit of the first three bytes is 1. It is now clear that the first two bytes are used to identify the class B network, the third byte is used to identify the subnet within this class B network, and the last byte is then the host number.

Not all IP addresses are available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zeros and all ones as the host number. For example, for an IP address of 128.1.2.128, what will the reserved IP addresses look like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask that is 25 bits long, 255.255.255.128, contains 126 members in the sub-netted network. Another concept to be remembered is that the length of the network prefix equals the number of the bits with 1s in that subnet mask. Using this information, the number of IP addresses matched can be easily counted. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-3

According to the scheme above, a subnet mask 255.255.255.0 will partition a class C network. It means there will be a maximum of 254 effective nodes existing in this sub-netted network and it is considered a physical network in an autonomous network. It therefore owns a network IP address which may look like 168.1.2.0.

Using subnet masking, a large network can be cut into smaller pieces of network. If we want to have more than two independent networks in an Enterprise network, a partition to the network must be performed. In this case, a subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as the default router. Basically, it is a routing policy. The gateway setting is used for Trap Events Host only in the switch.

To assign an IP address to the switch, to the administrator must check what the IP address is of the network that will be connected with the switch. Use the same network address and append your host address to it.

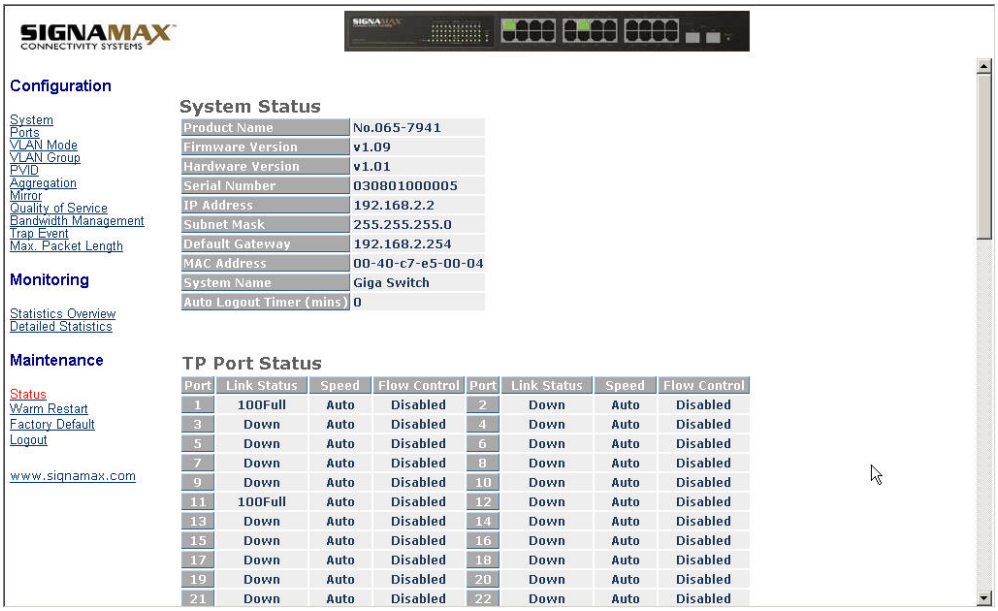


Fig. 2-9

First: IP Address: as shown in Fig. 2-9, enter “192.168.1.1”, for example. An IP address such as 192.168.1.x must be set on your PC to communicate with the switch.

Second: Subnet Mask: as shown in Fig. 2-9, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

2-2. Typical Applications

The 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch implements 24 Gigabit Ethernet TP ports with auto MDIX and two slots for the removable modules supporting comprehensive types of fiber optic connection, including LC and BiDi-LC SFP modules. For more details on the specifications of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central /Remote Site applications, as used in carriers or ISPs (See Fig. 2-10)
- Peer-to-peer applications, as used in two remote offices (See Fig. 2-11)
- Office networks (See Fig. 2-12)

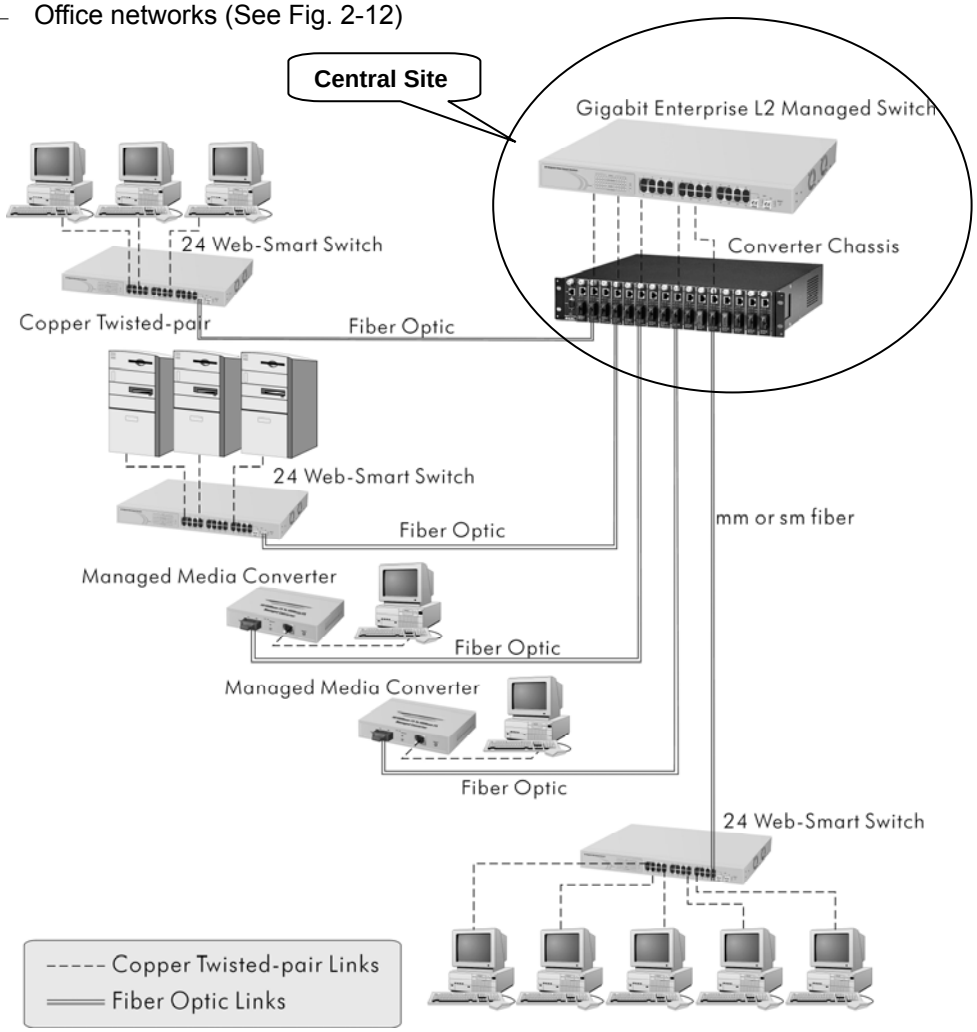


Fig. 2-10 Network Connection between Remote Site and Central Site

Fig. 2-10 is a system-wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

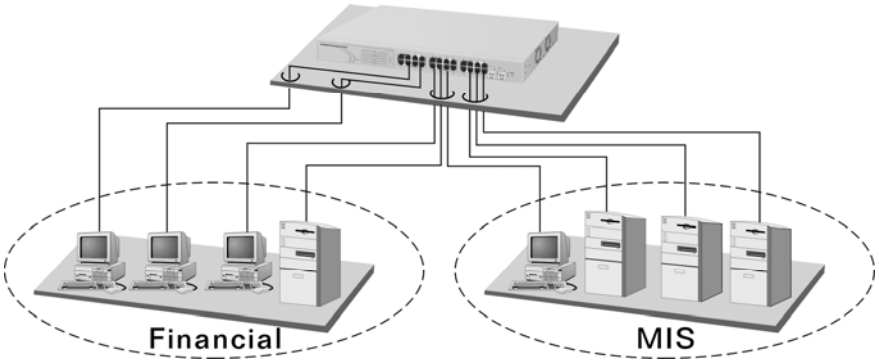


Fig. 2-11 Peer-to-peer Network Connection

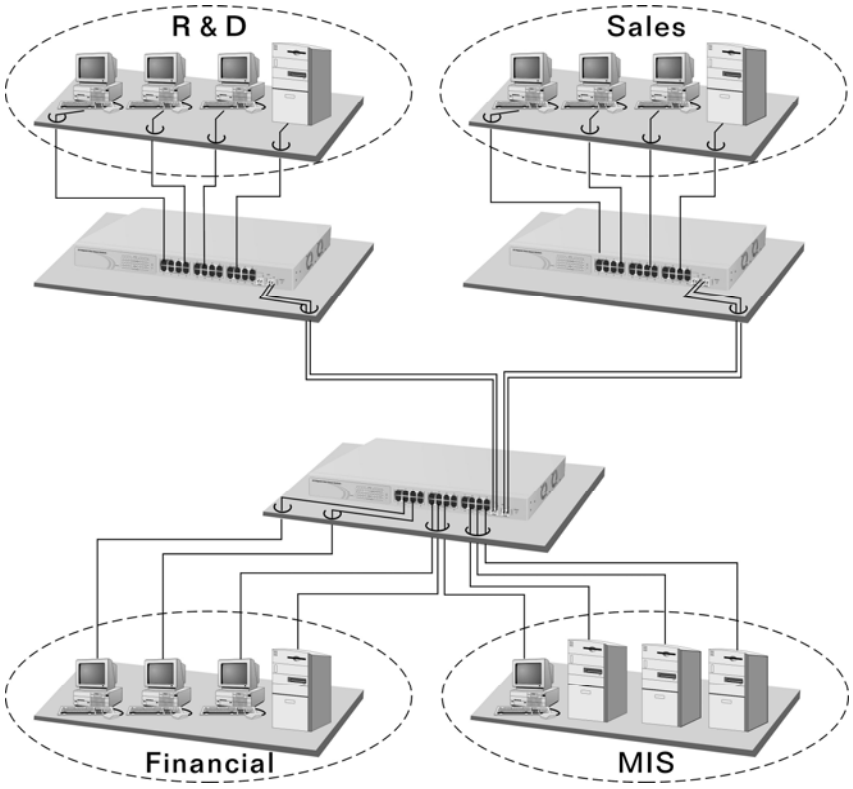


Fig. 2-12 Office Network Connection

3. Basic Concept and Management

This chapter will tell you the basic concept of features to manage this switch and how they work.

3-1. What's Ethernet?

Ethernet originated and was implemented at Xerox in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high speed Ethernet with the same characteristic of the original Ethernet but operated at 100 Mbps, now called Fast Ethernet. This means Fast Ethernet inherits the same frame format, CSMA/CD, software interface. In 1998, Gigabit Ethernet was rolled out and provided 1000 Mbps. Now 10G/s Ethernet is in the approval process. Although these Ethernet architectures have different speeds, they still use the same basic functions. Therefore, they are compatible in software and can connect to each other almost without limitation. The transmission media may be the only concern.

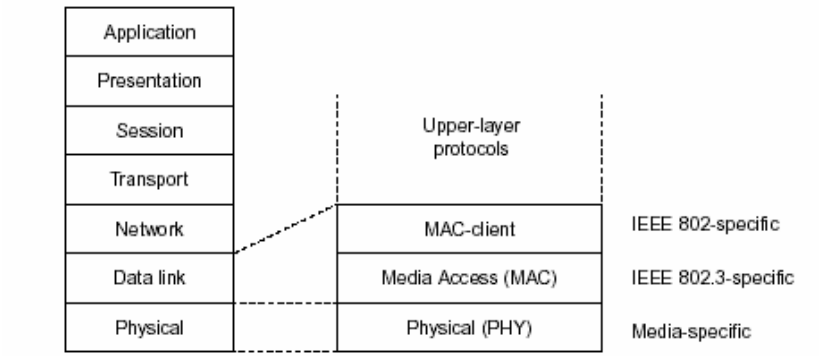
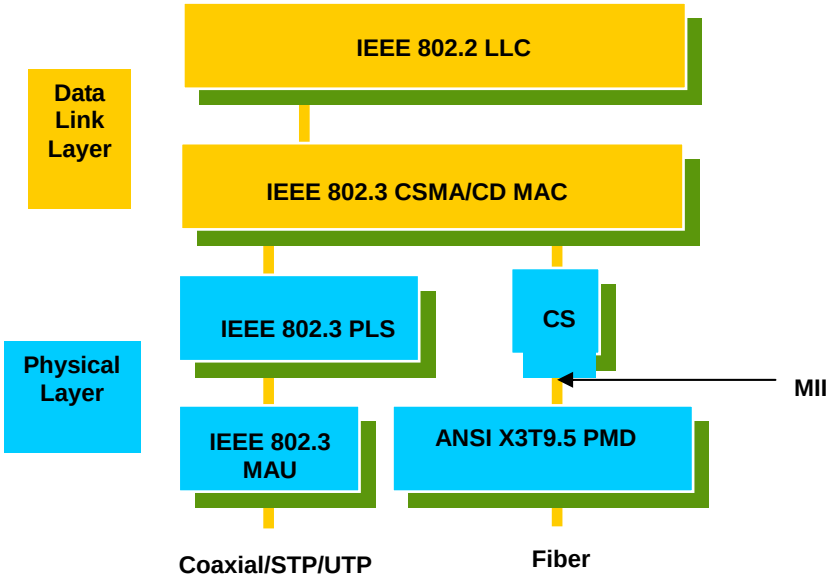


Fig. 3-1 IEEE 802.3 reference model vs. OSI reference mode

In Fig. 3-1, we can see that Ethernet is located at the Data Link layer and Physical layer and is comprised of three portions, including logical link control (LLC), media access control (MAC), and the physical layer. The first two portions comprise the Data link layer, which performs the functions of splitting data into frames for transmitting, receiving acknowledgement frames, error checking and re-transmitting when not received correctly, as well as providing an error-free channel upward to the network layer.



The diagram above shows the Ethernet architecture, LLC sub-layer, and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are correspond to the Physical layer in the OSI model. In this section, we are mainly describing the MAC sub-layer.

Logical Link Control (LLC)

The Data Link layer is composed of both of the sub-layers of the MAC and the MAC-client. Here the MAC client may be a logical link control or bridge relay entity.

Logical link control supports the interface between the Ethernet MAC and the upper layers in the protocol stack, usually the Network layer, which has nothing to do with the nature of the LAN. Therefore, it can operate over other different LAN technologies such as Token Ring, FDDI and so on. Likewise, for the interface to the MAC layer, LLC defines the services with the interface independent of the medium access technology and with some of the nature of the medium itself.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

DSAP address	=	Destination service access point address field
SSAP address	=	Source service access point address field
Control	=	Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
Information	=	Information field
*	=	Multiplication
M	=	An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

Table 3-1 LLC Format

Table 3-1 is the format of the LLC PDU. It is comprised of four fields: DSAP, SSAP, Control and Information. The DSAP address field identifies one or more service access points, in which the I/G bit indicates if it is an individual or group address. If all bits of the DSAP are 1s, it is a global address. The SSAP address field identifies the specific services indicated by the C/R bit (command or response). The DSAP and SSAP pair with some reserved values to indicate some well-known services listed in the table below.

0xAAAA	SNAP
0xE0E0	Novell IPX
0xF0F0	NetBIOS
0xFEFE	IOS network layer PDU
0xFFFF	Novell IPX 802.3 RAW packet
0x4242	STP BPDU
0x0606	IP
0x9898	ARP

Table 3-2

LLC type 1 connectionless service, LLC type 2 connection-oriented service and LLC type 3 acknowledge connectionless service are three types of LLC frames used for all classes of service. In Fig 3-2, the format of the Service Access Point (SAP) is shown). Please refer to IEEE 802.2 for more details.

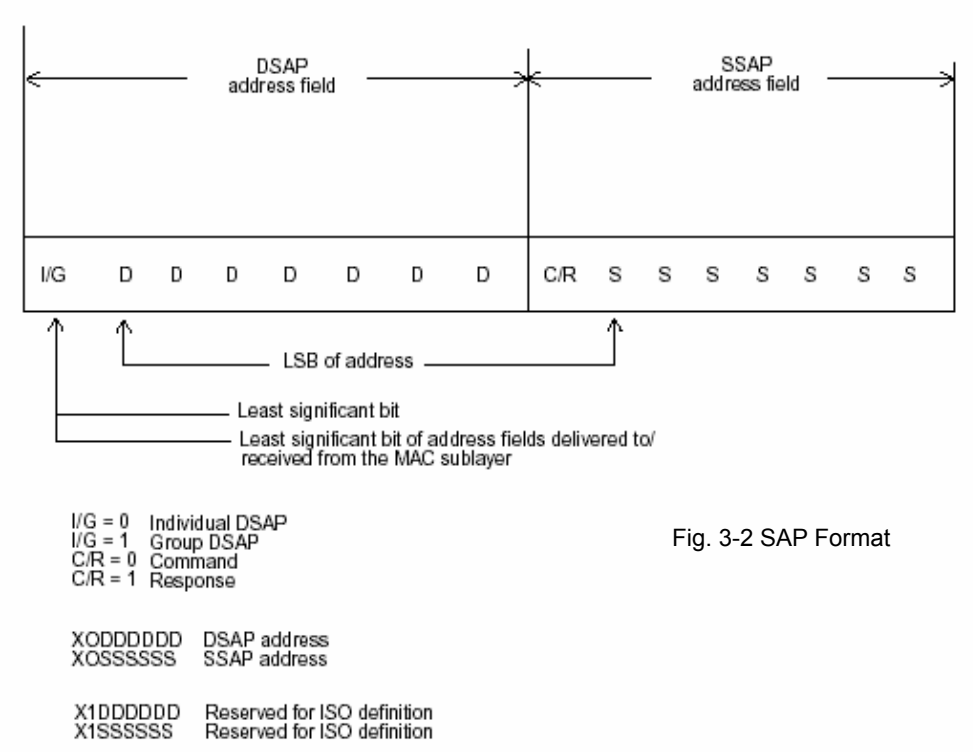

DSAP
address field
SSAP
address field
I/G D D D D D D D
C/R S S S S S S S
LSB of address
Least significant bit
Least significant bit of address fields delivered to/
received from the MAC sublayer
I/G = 0 Individual DSAP
I/G = 1 Group DSAP
C/R = 0 Command
C/R = 1 Response
XODDDDDD DSAP address
XOSSSSSS SSAP address
X1DDDDDD Reserved for ISO definition
X1SSSSSS Reserved for ISO definition

Fig. 3-2 SAP Format

3-2. Media Access Control (MAC)

MAC Addressing

Because a LAN is composed of many nodes, for the data exchanged among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In the OSI model, each layer provides its own means to identify the unique address in some form; for example, an IP address in the network layer.

The MAC belongs to the Data Link Layer (Layer 2); the address is defined to be a 48-bit long and locally unique address. Since this type of address is applied only to the Ethernet LAN media access control (MAC), they are referred to as MAC addresses.

The first three bytes are Organizational Unique Identifier (OUI) code assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All six of these bytes are stored in a non-volatile memory in the device. Their format is as shown in the following table and normally written in the form as aa-bb-cc-dd-ee-ff, a sequence of 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by the manufacturer.

Bit 47					bit 0
1st byte	2nd byte	3rd byte	4th byte	5th byte	6th byte
OUI code			Serial number		

Table 3-3 Ethernet MAC address

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as an I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for global-unique (0) or locally-unique addresses. The former is assigned by the device manufacturer, and the latter is usually assigned by the administrator. In practice, global-unique addresses are always applied.

A unicast address is identified with a single network interface. With this type of MAC address, a frame transmitted can be received by exactly the target interface the destination MAC points to.

A multicast address is identified with a group of network devices or network interfaces. In Ethernet, a means of many-to-many connectivity in the LANs is provided. It provides a method of sending a frame to many network devices at a time. When all bits of a DA are 1s, it is a broadcast, which means all network devices except the sender itself can receive the frame and respond.

Ethernet Frame Format

There are two major forms of Ethernet frames, type encapsulation and length encapsulation, both of which are categorized as four frame formats 802.3/802.2 SNAP, 802.3/802.2, Ethernet II and Netware 802.3 RAW. We will introduce the basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations. It contains seven fields as explained below.

PRE	SFD	DA	SA	Type/Length	Data	Pad bit if any	FCS
7	7	6	6	2	46-1500		4

Fig. 3-3 Ethernet frame structure

- **Preamble (PRE)** —The PRE is 7-byte long with alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

  10101010 10101010 10101010 10101010 10101010 10101010 10101010

- **Start-of-frame delimiter (SFD)** — The SFD is one-byte long with an alternating pattern of ones and zeros, ending with two consecutive 1-bits. It immediately follows the preamble and uses the last two consecutive 1 bits to indicate that the next bit is the start of the data packet and the left-most bit in the left-most byte of the destination address. The SFD pattern is 10101011.

- **Destination address (DA)** — The DA field is used to identify which network device(s) should receive the packet. It is a unique address. Please see the section concerning MAC addressing.

- **Source addresses (SA)** — The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.

- **Length/Type** — This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal, the number of bytes in the data field is equal to the Length/Type value, i.e. this field acts as Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation and Netware 802.3 RAW encapsulation. Each of them has different fields following the Length field.
- If the Length/Type value is greater than 1500, it means the Length/Type acts as Type. Different type value means the frames with different protocols running over Ethernet being sent or received.

For example,

0x0800	IP datagram
0x0806	ARP
0x0835	RARP
0x8137	IPX datagram
0x86DD	IPv6

- **Data** — Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend the padding bits and have the payload be equal to 46 bytes. The length of data field must equal the value of the Length field when the Length/Type acts as Length.

- **Frame check sequence (FCS)** — This field contains a 32-bit cyclic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

- It is created by the sending MAC and recalculated by the receiving MAC to check if the packet is damaged or not.

How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. *Receiving and transmitting data*. When receiving data, it parses frames to detect errors; when transmitting data, it performs frame assembly.
2. *Performing Media access control.* It prepares the initiation jobs for a frame transmission and facilitates recovery from transmission failure.

Frame transmission

As Ethernet adopted Carrier Sense Multiple Access with Collision Detect (CSMA/CD) as its operating protocol, it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also “Listen”. If there is signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first, then the next, Start of Frame Delimiter (SFD), DA, SA and through the data field and FCS field in turn. The following summarizes what a MAC does before transmitting a frame.

1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, either type or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.
2. Listen if there is any traffic running over the medium. If yes, wait.
3. If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, i.e. inter-frame gap time to have the MAC ready with enough time and then start transmitting the frame.
4. During the transmission, MAC keeps monitoring the status of the medium. If no collision happens until the end of the frame, it transmits successfully. If there is a collision happened, the MAC will send the patterned jamming bit to guarantee the collision event is propagated to all involved network devices, then wait for a random period of time, i.e. backoff time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempt reaches 16 times, the frame in the MAC’s queue will be discarded.

An Ethernet MAC transmits frames in half-duplex and full-duplex modes. In the half-duplex operation mode, the MAC can either transmit or receive a frame at a given moment, but cannot do both jobs at the same time.

As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the frame, in the worst case, just before the frame from the first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in a 10 Mbps LAN, it's 2500 meters, in a 100 Mbps LAN, it's approximately 200 meters and in 1000 Mbps, 200 meters. According to the theory, it should be 20 meters. But it's not practical, so the LAN diameter is maintained by increasing the minimum frame size with a variable-length non-data extension bit field which is removed at the receiving MAC. The following tables are the frame formats suitable for 10 M, 100 M and 1000 M Ethernet, and some parameter values that shall be applied to all of these three types of Ethernet.

Actually, the currently-available Gigabit Ethernet chips do not feature this so at this time. They all have their chips supported in the full-duplex mode only, and this applies to all network vendors' devices as well. So, this criterion should not exist at the present time or in the future. The switch's Gigabit modules support only the full-duplex mode.

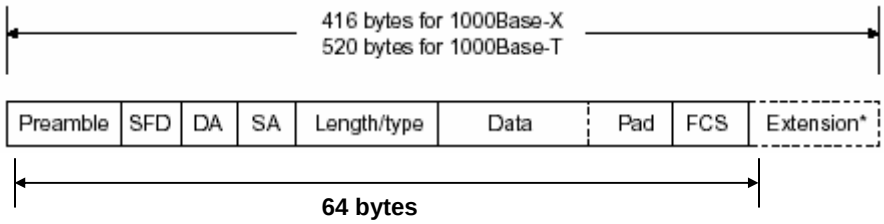
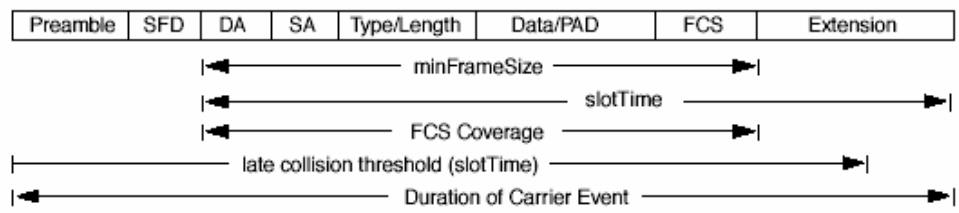


Fig. 3-4 Gigabit Ethernet Frame

Parameter value/LAN	10Base	100Base	1000Base
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe Gap	9.6us	0.96us	0.096us
AttemptLimit	16	16	16
BackoffLimit	10	10	10
JamSize	32 bits	32 bits	32 bits
MaxFrameSize	1518	1518	1518
MinFrameSize	64	64	64
BurstLimit	Not applicable	Not applicable	65536 bits

Table 3-4 Ethernet parameters for half duplex mode



In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule, or padding bits for short frames. The rest of the functions follow the specification of IEEE 802.3. For example, it must meet the requirement of minimum inter-frame gap between successive frames and frame format the same as that in the half-duplex mode of operation.

Because no collisions will happen in full-duplex operation, there is no mechanism to tell all the involved devices if frames are properly received. What will the situation be if the receiving device is busy and a frame is coming at the same time? Can it use “backpressure” to tell the source device to refrain from transmitting? Because of these issues, a flow control function is introduced in the full-duplex mode of operation.

3-3. Flow Control

Flow control is a mechanism used to tell the source device to stop sending frames for a specified period of time designated by the target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from the target device to the source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to the source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical to the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. Per the specification, the PAUSE operation can not be used to inhibit the transmission of MAC control frames.

Normally, in 10 Mbps and 100 Mbps Ethernet, only symmetric flow control is supported. However, some switches (e.g., the 065-7941 Gigabit WebSmart Switch) support not only symmetric but asymmetric flow controls for special applications. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting a PAUSE frame in one way from one side, and the other side is not allowed to transmit but can only receipt-and-discard the flow control information. Symmetric flow control allows both two ports to transmit PAUSE frames to each other simultaneously.

Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to have the medium clear and stabilized as well as to have the jobs ready, such as adjusting buffer counter, updating counter and so on, in the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In IEEE 802.3 specification, this is 96 bit times or more.

Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision always occurs and interferes with each other. This results the carrier signal becoming distorted and un-discriminated. MAC devices can detect, through the physical layer, the distortion of the carrier signal. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continues transmitting until the rest of the bits specified by the jamSize parameter are completely transmitted. This guarantees the duration of the collision is long enough to have all involved devices able to detect the collision. This is referred to as Jamming. After the jamming pattern is sent, the MAC stops transmitting the rest of the data queued in the buffer and waits for a random period of time, known as backoff time, with the following formula. When backoff time expires, the device goes back to the state of attempting to transmit the frame. The backoff time is determined by the formula below. When the times of collision are increased, the backoff time gets longer until the number of collisions exceed 16. If this happens, the frame will be discarded and the backoff time will also be reset.

$$0 \le r < 2^k$$

where

k = min (n, 10)

Frame Reception

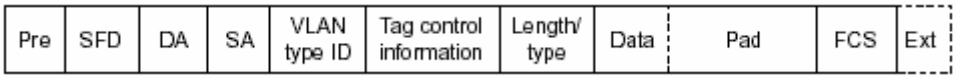
In essence, the frame reception is the same in both half duplex and full duplex operations, except that full-duplex operation uses two buffers to transmit and receive the frames independently. The receiving node always “listens” if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes, the receiver of the target device begins receiving the bit stream, and looks for the PRE (Preamble) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame until all bit of the frame is received.

For a received frame, the MAC will check:

1. If it is less than one slotTime in length, i.e. short packet, and if yes, it will be discarded by the MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, it means there may be a collision that has happened somewhere or an interface malfunctioned in the LAN. When detecting this, the MAC drops the packet and goes back to the ready state.
2. If the DA of the received frame exactly matches the physical address that the receiving MAC owns or the multicast address designated to recognize. If not, the MAC discards it and the MAC passes the frame to its client and goes back to the ready state.
3. If the frame is too long. If yes, throws it away and reports frameTooLong.
4. If the FCS of the received frame is valid. If not, for 10 M and 100 M Ethernet, the MAC discards the frame. For Gigabit Ethernet or higher speed Ethernet, the MAC has to check one more field, i.e. extra bit field, if the FCS is invalid. The MAC also checks if there are any extra bits existing, which must meet the specification of IEEE 802.3. When both FCS and extra bits are valid, the received frame will be accepted; otherwise, the MAC discards the received frame and reports frameCheckError if no extra bits were appended or alignmentError if extra bits were appended.
5. If the length/type is valid. If not, the MAC discards the packet and reports lengthError.
6. If all five procedures above are OK, then the MAC treats the frame as good and de-assembles the frame.

What if a VLAN tagging is applied?

VLAN tagging is a 4-byte long data string immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will have a little change, shown as follows.



Only two fields, VLAN ID and Tag control information, are different in comparison with the basic Ethernet frame. The rest of the fields are the same.

The first two bytes are the VLAN type ID with the value of 0x8100 indicating the received frame is a tagged VLAN frame, and the next two bytes are Tag Control Information (TCI), used to provide user priority, and VLAN ID, which are explained respectively in the following table.

Bits 15-13	User Priority 7-0, 0 is lowest priority
Bit 12	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header 0: No RIF field is present
Bits 11-0	VID (VLAN Identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFF: Reserved

Table 3-5

Note: RIF is used in Token Ring network to provide source routing and comprises two fields, Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports that are associated with that VID. If it happens in a network interface card, the MAC will deprive the frame of the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with the optional VLAN function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, as this would have deleterious effects. Nondata bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

3-4. How does a switch work?

The 065-7921 Gigabit WebSmart switch is a layer 2 Ethernet Switch equipped with 22 10/100/1000 Mbps Twisted Pair (TP) ports and 2 Gigabit dual media TP/SFP (Small Form-factor Pluggable) fiber ports . Each port on it is an independent LAN segment and thus has 24 LAN segments and 24 collision domains, in contrast to the traditional shared Ethernet hub in which all ports share the same media and use the same collision domain and thus limit the bandwidth utilization. With the switch's separated collision domains, it can extend the LAN diameter farther than a shared hub does and highly improve the efficiency of the traffic's transmission.

Due to this architecture, the switch can provide full-duplex operation to double the bandwidth per port and provide many other features, such as VLAN, bandwidth aggregation and so on, that are not able to be supported in a shared hub.

Terminology

Separate Access Domains:

As described in the section of "What's Ethernet?", Ethernet utilizes CSMA/CD to arbitrate who can transmit data to the station(s) attached in the LAN. When more than one station transmits data within the same slot time, the signals will collide, referred to as collision. The arbitrator will arbitrate who should gain the media. The arbitrator is a distributed mechanism in which all stations contend to gain the media. Please refer to the "What's Ethernet?" section for more details.

In Fig.3-5, assumed as half duplex, you will see some ports of the switch are linked to a shared hub, which connects many hosts, and some ports just are individually linked to a single host. The hosts attached to a shared hub will be in the same collision domain, separated by the switch, and use CSMA/CD rule. For the host directly attached to the switch, because no other host(s) joins the traffic contention, hence it will not be affected by CSMA/CD. These LAN segments are separated in different access domains by the switch.

Micro-segmentation:

To have a port of the switch connected to a single host is referred to as micro-segmentation. It has the following interesting characteristics.

- There is no need for the access contention (e.g.Collision). They have their own access domain. But, collision still could happen between the host and the switch port.
- When performing in the full duplex mode, the collision vanishes.
- The host owns a dedicated bandwidth of the port.

The switch port can run at different speed, such as 10 Mbps, 100 Mbps or 1000 Mbps. A shared hub cannot offer this capability.

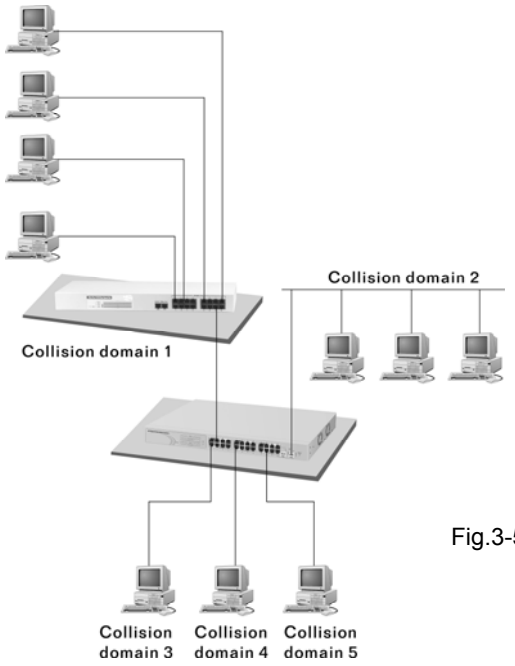


Fig.3-5 Collision Domain

Extended Distance Limitations:

The diameter of a half-duplex LAN segment is determined by its maximum propagation delay time. For example, in 10 M LAN, the maximum distance of a LAN segment using yellow “Thicknet” cable is 2500 meters and 185 meters when using coaxial “Thinnet” cable. The switch with its collision domain per port can extend the distance as a bridge does. Furthermore, when operating in full-duplex mode, the distance can reach farther than half duplex because it is not limited by the maximum propagation delay time (512 bits time). If fiber media is applied in the network, the distance can be up to tens of kilometers.

Traffic Aggregation:

Traffic aggregation is used to aggregate the bandwidth of more than one port and treat it as a single port in the LAN. This highly increases the total available bandwidth to the targeted device. This is a great feature for the port needing more bandwidth where the cost for a high bandwidth port is prohibitive.

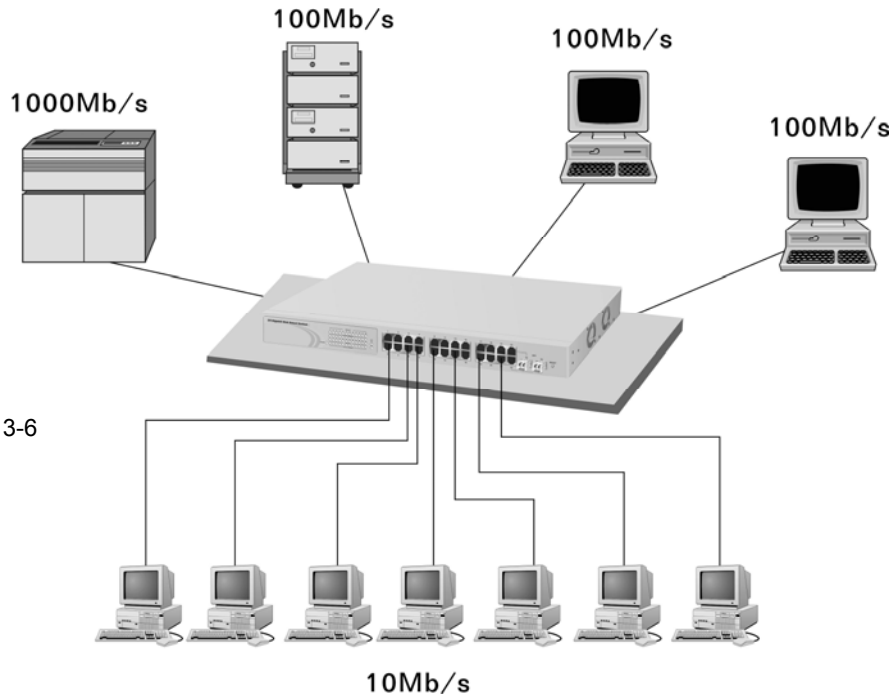


Fig. 3-6

How does a switch operate?

A Layer 2 switch uses some features of the Data Link layer in the OSI model to forward the packet to the destination port(s). Here we introduce some important features of a switch and how they work.

MAC address table

When a packet is received on a port of switch, the switch first checks if the packet is good or bad and extracts the source MAC address (SA) and destination MAC address (DA) to find 1) if SA is existing in the MAC address table; if no, the switch puts it in the MAC address table; if yes, 2) looks up DA and its associated port to which the traffic is forwarded. If the DA does not exist, the switch will have the packet broadcasted.

Due to the size of the MAC address table being limited, a MAC address aging function is applied. When the MAC address has resided and has not been updated in the table for a long time, this means that traffic using that entry has not arrived for a while. If this time period is more than the aging time, the entry will be marked invalid. The vacancy is now available for other new MAC addresses.

Both learning and forwarding are the most important functions in a switch. Besides that, VLAN can be one of the rules to forward the packet. There are ingress rules and egress rules applied. The ingress rule is used to filter the incoming packet by VLAN ID and so on and to decide whether the packet is allowed to enter the switch or not. The egress rule is used to forward the packet to the proper port.

MAC address aging

There is a field in the MAC address table used to establish the entry's Age time, which determines how long a MAC entry can reside in a switch. The age time is refreshed when a packet with that SA is received. Usually, the age time is programmable.

Transmission schedule

In most layer 2 switches, the QoS function is supported. QoS in a switch must associate a transmission schedule to transmit the packet. This function has much to do with the priority level a packet has. With the given priority, the scheduler will perform the proper action upon it. The scheduler has many ways to be implemented, and different chips may support different scheduling algorithms. The most common schedulers are:

FCFS: First Come, First Service.

Strictly Priority: All High before Low.

Weighted Round Robin:

Set a weight figure to the packet with a given priority level, say 5-7, and next, set another weight to the packet with a different priority level, say 2-4 and so on. The WRR scheduler will transmit the packet, taking the weight into account. Therefore, packets of each priority level can be allocated a fixed bandwidth.

Bandwidth rating

Bandwidth rating is the limitation set by administrator, and it can be applied to those with SLA. Bandwidth rating can be total bandwidth, or types of service of a port with many steps. The switch supports by-port Ingress and Egress total bandwidth rate control capacity. The bandwidth rate resolution is 0.1 Mbps (100 Kbps) and ranges from 0 to 100 Mbps.

3-5. Virtual LAN

What is a VLAN?

It is a subset of a LAN. Before we discuss VLAN, we must understand what a LAN (Local Area Network) is. In general, a LAN is composed of different physical network segments bridged by switches or bridges which attach to end stations in the same broadcast domain. The traffic can reach any station on the same LAN. Beyond this domain, the traffic cannot be sent without the help of a router. This also implies that a LAN is limited. If you need to communicate with the station outside the LAN, a router is needed, which always lies on the edge of the LAN.

For a layer 2 VLAN, it assumes it is a logical subset of a physical LAN separated by specific rules such as tag, port, MAC address and so on. In other words, they can communicate with each other between separated small physical LANs within a LAN but can not be between any two separated logical LANs.

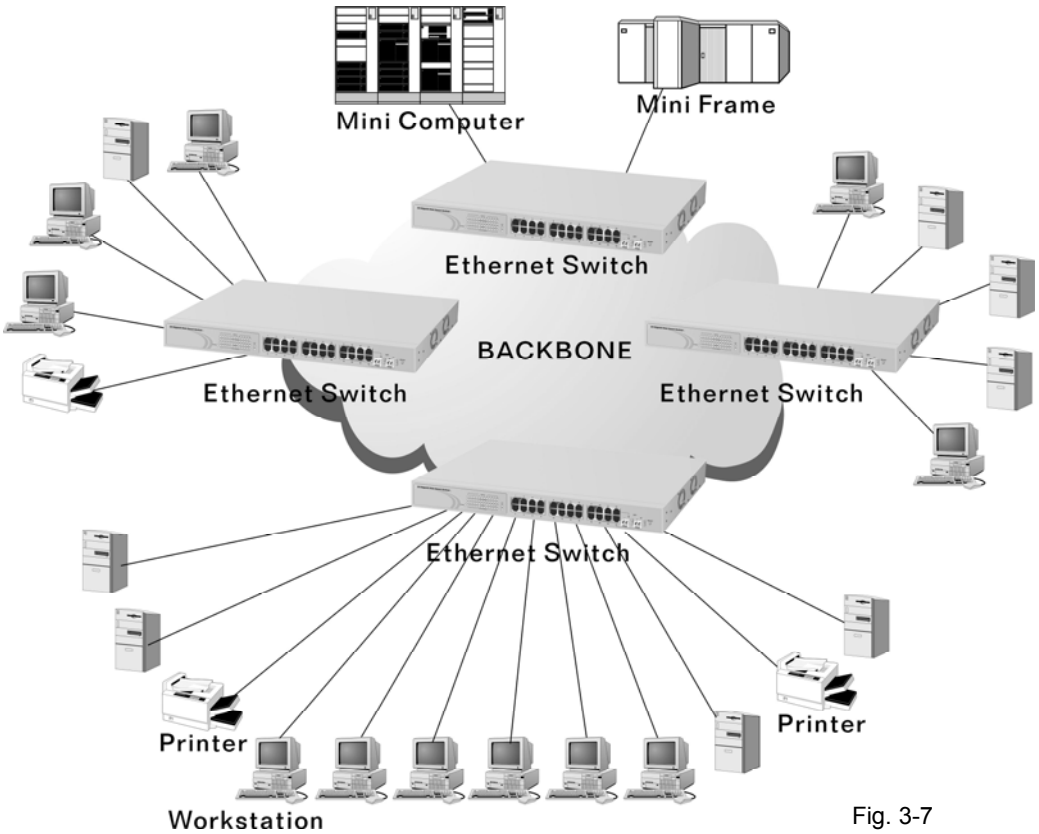


Fig. 3-7

In the figure above, all stations are within the same broadcast domain. For these stations, it is obvious that the traffic is getting more congested as more stations are added to it. With the more and more users joining the LAN, the performance of the network will rapidly deteriorate due to increased broadcast traffic . In the worst case, the network may go down completely.

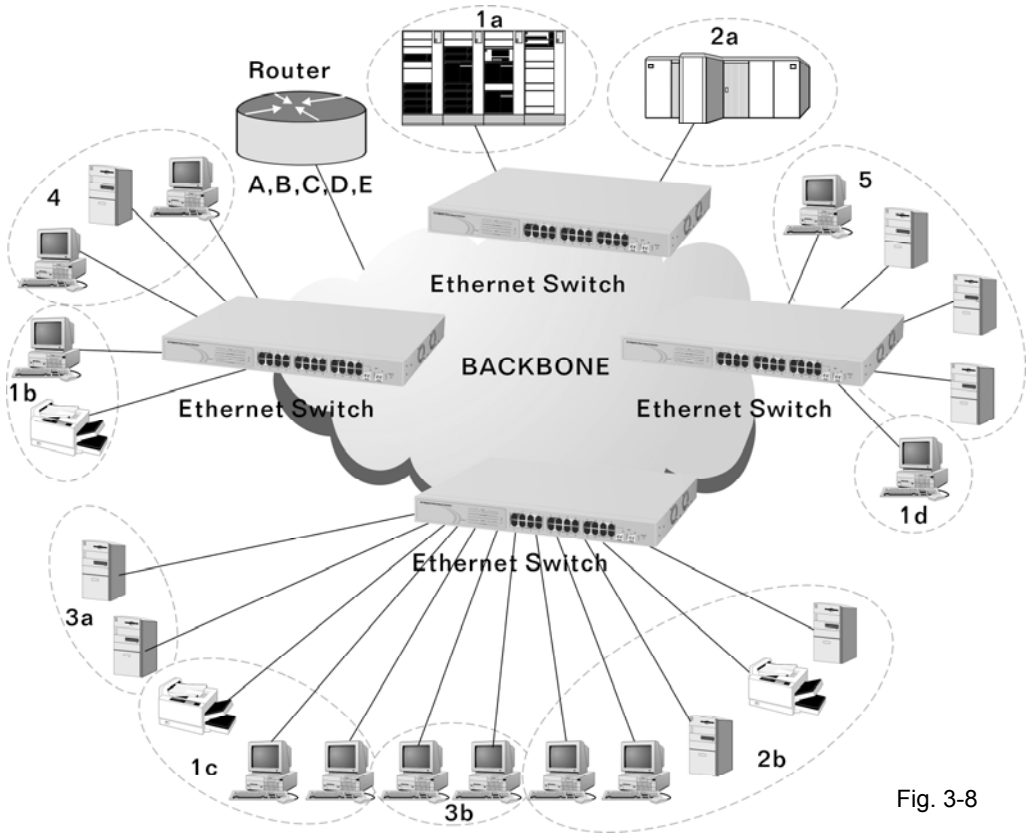


Fig. 3-8

In this diagram, VLAN technology is applied to configure the system as shown as the figure above. We can partition the users into the different logical networks which have their own broadcast domain. The traffic in one VLAN will not disturb others of these logical networks. The users 1x (x denotes a ~ d) are members of VLAN 1. Any traffic within VLAN 1 does not flow to VLAN 2 or any others. This helps the administrator to configure the network easily according to the criteria needed, for example, financial, accounting, R&D, and whatever else might be necessary. You can also easily move a user to a different location or have a new user somewhere in the building join the VLAN. Without VLAN, it is very hard to do. Fundamentally, the use of VLAN offers at least 3 benefits: easier movement and change of the users, reduced broadcast traffic that improves performance within a broadcast domain, and improved security.

In addition, VLANs can highly reduce the traffic congestion between LANs and increase overall network performance because there are no longer too many users in the same broadcast domain.

There are many types of VLAN that can be applied to a LAN. The most popular types are port-based VLAN, tag-based VLAN and protocol-based VLAN.

- Port-based VLAN

  Some physical ports are configured as members of a VLAN. All stations attached on these ports can communicate with each other.

- Tag-based VLAN

  Tag-based VLAN identifies the membership by VLAN ID, no matter where the packet comes from. It is also referred to as 802.1Q VLAN.

- Protocol-based VLAN

  Protocol-based VLAN identifies the VLAN membership by layer 3 protocol types, for example IPX, AppleTalk, IP, etc.

Other VLAN technologies not mentioned above are MAC-based VLAN, IP-based VLAN, and so on.

Terminology

Tagged Frame:

A frame, carrying a tag field following the source MAC address, is four bytes long and contains VLAN protocol ID and tag control information composed of user priority, Canonical Format Indicator (CFI) and optional VLAN identifier (VID). Normally, the maximum length of a tagged frame is 1522 bytes.

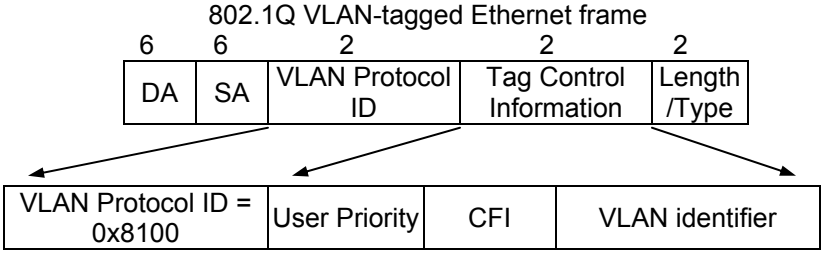


Fig.3-9 Tag Format

VLAN Protocol ID: 8100 is reserved for VLAN-tagged frame.

User Priority: 3 bits long. User priority is defined to a range of 7 – 0. 0 is the lowest priority.

CFI: Canonical Format Indicator. 1 bit long. It is used to encapsulate a token ring packet to let it travel across the Ethernet. Usually, it is set to 0.

VLAN ID: 12 bits long. 0 means no VLAN ID is present. 1 means the default VLAN, 4095 reserved.

VLAN-tagged frame:

An Ethernet frame, carrying a VLAN tag field, containing VLAN identification without the values of 0 and 4095, and priority information.

Priority-tagged frame:

An Ethernet frame, carrying a VLAN tag field, containing VLAN identification with the value of 0, and priority information.

Untagged frame:

An Ethernet frame carrying no VLAN tag information.

VLAN Identifier:

Also referred to as VID. It is used to identify a member belonging to the VLAN group with the VID. The assignable number is 1- 4094. If VID=0, the tagged frame is a priority packet. Neither of the values of 0 and 4095 can be assigned in VLAN management.

Port VLAN Identifier:

VLAN identifier of a port. It also can be referred to as PVID. When an untagged frame or a priority-tagged frame is received, the frame will be inserted the PVID of that port in the VLAN tag field. The frame with VID assigned by a port is called PVID. Each port can only be assigned a PVID. The default value for PVID is 1, the same as VID.

Ingress filtering:

The process used to check a received packet and compare its VID to the VLAN membership of the ingress port. The ingress filtering can be set by per port. When receiving a packet, a VLAN bridge examines if the VID in the frame's header has been presented.

If the VID of the received packet is presented, the VID of the packet is used. And the VLAN bridge will check its MAC address table to see if the destination ports are members of the same VLAN. If both are members of the tagged VLAN, then the packet will be forwarded.

If the packet is an untagged or a null tag packet, the ingress port's PVID is applied to the packet. The VLAN bridge will then look up the MAC address table and determine to which ports the packet should be forwarded. Next, it will check to see if the destination ports belong to the same VLAN with that PVID. If the destination ports are members of the VLAN used by the ingress port, the packet will be forwarded.

Note: VID can not be 0 or 4095.

Ingress Rule:

Each packet received by a VLAN-aware bridge will be classified to a VLAN. The classification rule is described as follows.

1. If the VID of the packet is null VID (VID=0), or this packet is an untagged packet:
   a. If there are still some other ways (e.g. protocol, MAC address, application, IP-subnet, etc.) to classify the incoming packets beside port-based classification implemented and these approaches can offer a non-zero VID, then use the value of VID offered by the other classifications for this VLAN's classification.
   b. If there is only port-based classification implemented or other classification approaches cannot offer a non-zero VID for the incoming packets, then assign the PVID to the incoming packets as VID for the classification of the VLAN group.
2. If the VID is not a null VID (VID≠0), then use the value to classify the VLAN group.

Egress Rule:

An egress list is used to make the tagging and forwarding decision on an outgoing port. It specifies the VLANs whose packets can be transmitted out and specifies if the packet should be tagged or not. It can be configured for the port's VLAN membership, and tagged or untagged for a transmitted packet. When a packet is transmitted out, the VLAN bridge checks the port's egress list. If the VLAN of the packet is on the egress list of the port on which the packet is transmitted out, the packet will be transmitted with the priority accordingly. If enabled, an egress port will transmit out a tagged packet if the port is connected to an 802.1Q-compliant device. If an egress port is connected to a non-802.1Q device or an end station, the VLAN bridge must transmit out an untagged packet, i.e. the tag has been stripped off in an egress port. Egress rule can be set on a per port basis.

Independent VLAN Learning (IVL):

It specifies the mode used to learn MAC addresses. For a specified VLAN, it will use an independent filtering database (FID) to learn or look up the membership information of the VLAN and decide where to go.

Shared VLAN Learning (SVL):

It specifies the mode used to learn MAC addresses. In this mode, some VLANs or all VLANs use the same filtering database, storing the membership information of the VLAN to learn or look up the membership information of the VLAN. In the 065-7941 switch, you can choose a VID for sharing the filtering database in the Shared VID field if you wish to use the existing filtering database. For a specified VLAN, when a MAC address is learned by a switch, the VLAN will use this information to make the forwarding decision.

Filtering Database:

Referred to as FID. It can provide the information regarding where the packet will be sent. The filtering database will supply the outgoing port according to the request from a forwarding process with VID and DA. When a packet is received, if it has a non-zero VID, then the FID will offer the associated outgoing ports information to the packet.

In SVL, VLANs use the same Filtering Database. In IVL, VLANs use different FIDs. Any VID can be assigned to the same FID by the administrator.

How does a Tagged VLAN work?

If ingress filtering is enabled and when a packet is received, the VLAN bridge will first check if the VID of the packet is presented.

1). If the packet has a non-zero VID, the VLAN bridge will apply this VID as the VLAN ID of the packet in the network.

2). For a packet with a null tag or no VLAN tag, if the VLAN bridge provides rules to decide its VID, then it will apply this VID to the packet.

If the VLAN bridge does not support any rule for VID, then apply the PVID of the port to the packet which came from that port. The VLAN bridge checks to see if the ingress port and the received packet are on the same VLAN. If not, it drops thee packet. If yes, it forwards the packet to the associated ports. Meanwhile, this VLAN must be applied to the egress port, or the packet will be dropped.

If ingress filtering is disabled, the VLAN bridge will only check the MAC address table to see if the destination VLAN exists. If the VLAN does not exist, it then drops the packet, and if both the DA and VLAN do not exist, forwards the packet. If it just knows VLAN existed, then it floods the packet to all the ports the VLAN covers.

If we plan to deploy four VLANs in an office and use a switch to partition them, we should check which ports belong to which VLAN first. Assuming a 24-port switch is used:

Name	VID	Port Members
Marketing	2	1,2,3,4,5
Service	3	6,7,20,21,22
Sales	4	8,9,10,11,12,13,14,15,16
Administration	1	17,18,19,23,24

Table 3-6

Next, the administrator assigns IP address to each VLAN. Usually, we use 10.x.x.x as internal IP block. Because there are total four VLANs in the network, we must assign 4 IP blocks to each of them.

Name	VID	Network Address
Marketing	2	10.1.2.0/24
Service	3	10.1.3.0/24
Sales	4	10.1.4.0/24
Administration	1	10.1.1.0/24

Table 3-7

Here we apply the subnet mask 255.255.255, and each VLAN is then capable of supporting 254 nodes.

3-6. Link Aggregation

The basic function of Link Aggregation is to aggregate the bandwidth of more than one port to an assigned logical link. This highly increases the total available bandwidth to the targeted device. There is more than one Link Aggregation technology in many vendors' switch products already, which may cause an interoperability problem. This is the reason why the 802.3ad Link Aggregation Control Protocol (LACP) standard was developed.

Why 802.3ad (LACP)?

Networks are constantly evolving and changing. For example, if a port malfunctioned or was accidentally unplugged in a static trunk port, the administrator has to reconfigure it, or the network will not operate properly. Therefore, offering a tool with automatic recovery capability is necessary for an administrator. LACP is a protocol that allows a switch to be able to know whether its partner has the capability to co-setup a trunk between them.

Usually, if the administrator wishes to increase the bandwidth of a specific link, he or she may:

1. Buy new network equipment with higher throughput, or
2. Aggregate the bandwidth of more than one port to a logical link.

If item 1 is the case, the solution's cost may exceed the budget, and the solution may not be scalable due to hardware limitations.

If item 2 is the case, costs are controlled and the existing equipment can flexibly accommodate to the new bandwidth demands associated with changes in the business. What's more, the interoperability issue is no longer a concern. By applying LACP in their network, a business reaps the benefits shown below of improving the performance of their network and saving funds that can be used to develop future products:

1. Public standardized specification
2. No interoperability issue
3. No change to IEEE 802.3 frame format, no change in software and management.
4. Increased bandwidth and availability
5. Load sharing and redundancy
6. Automatic configuration
7. Rapid configuration and reconfiguration
8. Deterministic behavior
9. Low risk of duplication or incorrect ordering
10. Support existing IEEE 802.3 MAC Clients
11. Backwards compatibility with aggregation-unaware devices

There are also some constraints when applying LACP.

1. LACP does not support inter-switch bandwidth aggregation.
2. The ports aggregated must operate in full-duplex mode.
3. The ports in the same Link Aggregation Group must have the same speed, for example, all with 100 Mbps or all 1000 Mbps. You cannot aggregate a 1000 Mbps link and two 100 Mbps links to create a 1.2 Gbps trunk port.

Terminology

Link Aggregation:

Link Aggregation is a method to have multiple physical links with the same media and speed bundled to be a logical link forming a Link Aggregation Group with a group ID. From the viewpoint of the MAC client, each Link Aggregation Group is an independent link.

There are three cases of links used in the network: switch to switch, switch to station and station to station. In this circumstance, a station may be a host or a router.

Link Aggregation, sometimes called port trunking, has two types of link configurations: static port trunk and dynamic port trunk.

- Static Port Trunk:

  When physical links are changed, the administrator needs to manually configure the switches one by one.

- Dynamic Port Trunk:

  When physical links are changed, LACP takes over and automatically reconfigures the links. The administrator does not have to do anything and may see the trap message of LACP changed in the NMS.

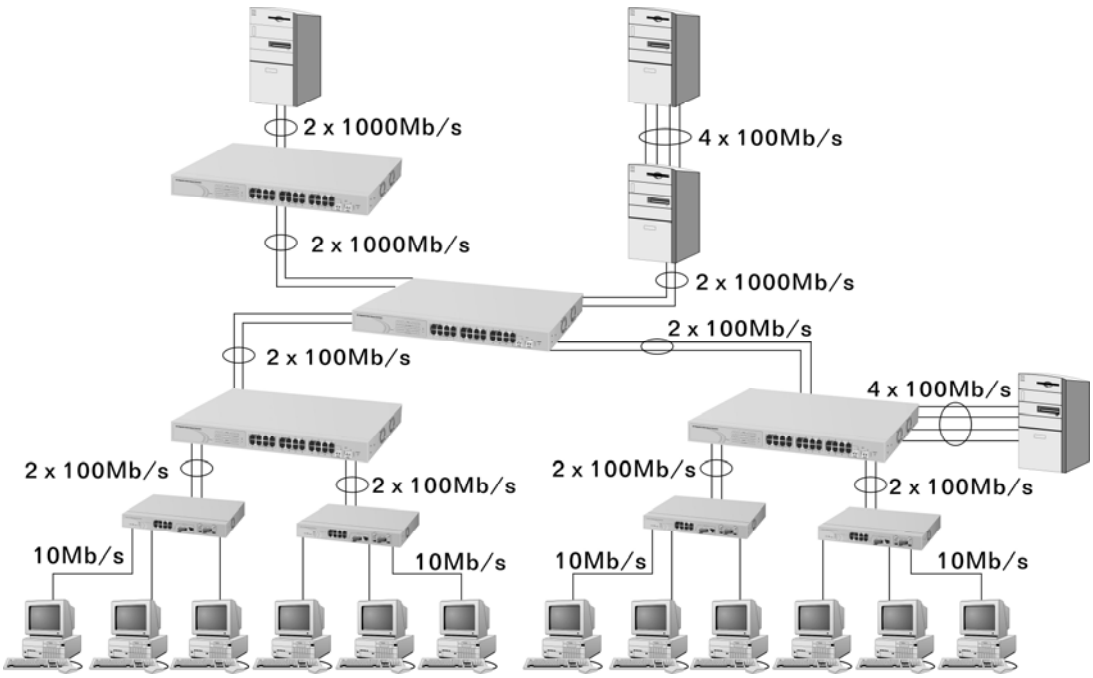


Fig. 3-10 Example of Link Aggregation Application

4. Operation of Web-based Management

This chapter instructs you how to configure and manage the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch through the web user interface it supports, in order to access and manage the 22 10/100/1000 Mbps TP ports and the 2 Gigabit TP/SFP dual media ports supporting either fiber or TP media in the switch. . With this facility, you can easily access and monitor through any one port of the switch all the statuses of the switch, including activity on each port, multicast traffic, and so on.

The default values of 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Password	admin

Table 4-1

After the 065-7941 24-Port 10/100/1000BaseT/TX WebSmart Switch has configured, the user can browse it by using the IP address the user has assigned to it. For instance, type http://192.168.1.1 in the address row in a browser, and it will show the following screen (see Fig.4-1) and request the user to input their password in order to login and access authentication. The default password is “admin”. When accessing the switch for the first time, please enter the default password, then click the **<Apply>** button. The login process is now completed.

This switch supports a simple user management function allowing only one administrator to configure the system at the same time.

To optimize the display, Signamax recommends that you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution set to 1024x768. The switch supports a neutral web browser interface.

The switch’s whole function tree that is capable of being administered using the web user interface is shown below, and will be discussed in detail in this chapter.

Fig. 4-1

4-1. Web Management Home Overview

After the user logs in, the switch displays the system status information as shown in Fig. 4-2. This page is the default page, providing the user with basic system information, including “System Status”, “TP Port Status”, “Fiber Port Status”, “Aggregation”, “VLAN”, “Mirror”, “Trap Event”, and “Maximum Packet Length”. With this information, the user will know the software version used, MAC address, how many ports are operating properly, and so on. This is helpful while troubleshooting the system. For more details, please refer to Section 4-4-1.

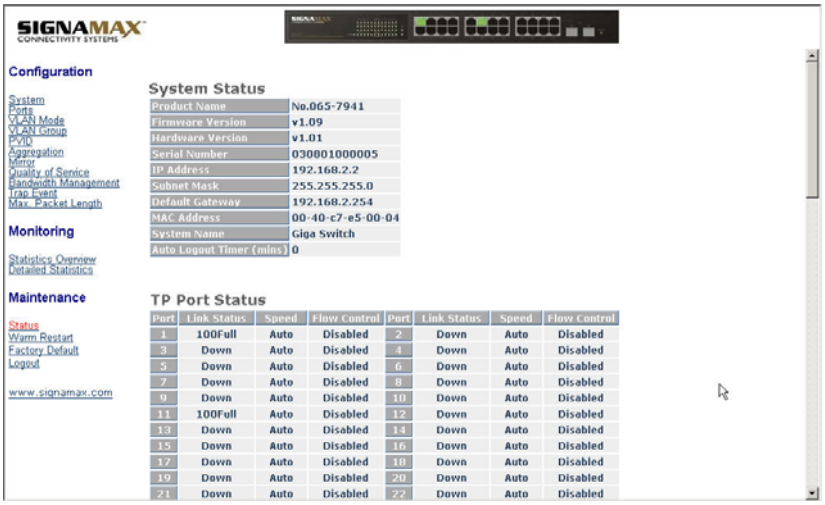
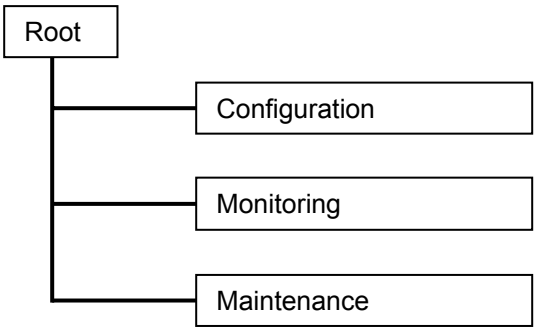


Fig. 4-2

• Page Layout Information

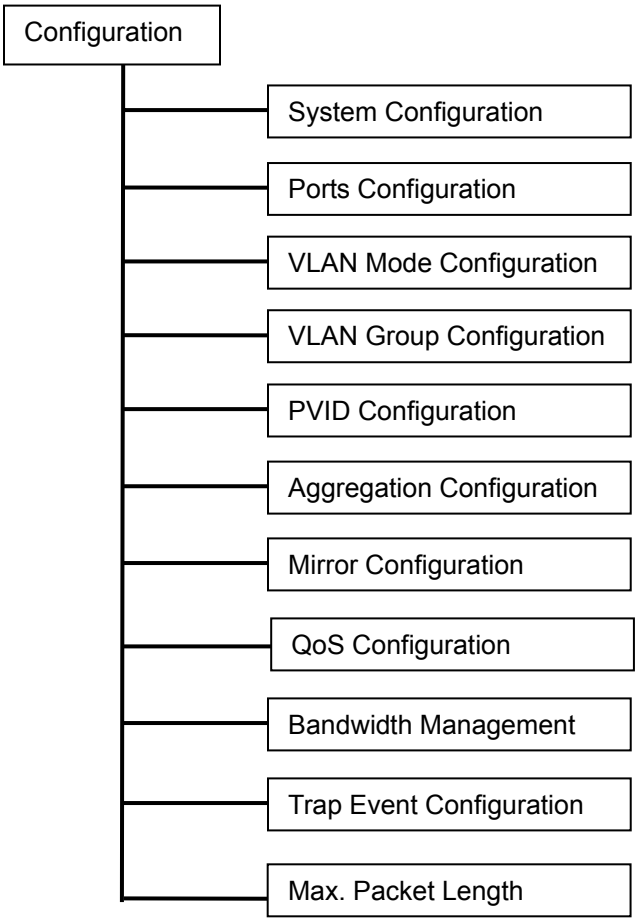
— On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; the ports which are not linked will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of the module depends on the one you inserted. The same link indications apply. If disconnected, the port will show as dark; if linked, the port will show as green.

— On the left side, the main menu tree for the web interface is listed in the page. They are hierarchical menus, with the function name in boldface. Open the function folder, and a sub-menu will be shown. All functions can be divided into three parts, including “Configuration”, “Monitoring” and “Maintenance”. The functions of each folder are described in their corresponding sections, respectively. The function is performed when mouse-clicked. The following list is the main function tree for the web-based user interface:



4-2. Configuration

Eleven functions, including System Configuration, Ports Configuration, VLAN Mode Configuration, VLAN Group Configuration, PVID Configuration, Aggregation Configuration, Mirror Configuration, QoS Configuration, Bandwidth Management, Trap Event Configuration, and Max. Packet Length are contained in this function folder for system and network management. Each of them will be described in detail in the following sections.



4-2-1. System Configuration

System configuration is one of the most important configurations in the switch. Without the proper setting, the network administrator, referred to here as the user, will not be able to manage or view the device. The switch supports manual IP address setting. When the IP address is changed, the user must reboot the switch to have the setting take effect and be able to use the new IP to browse for web management.

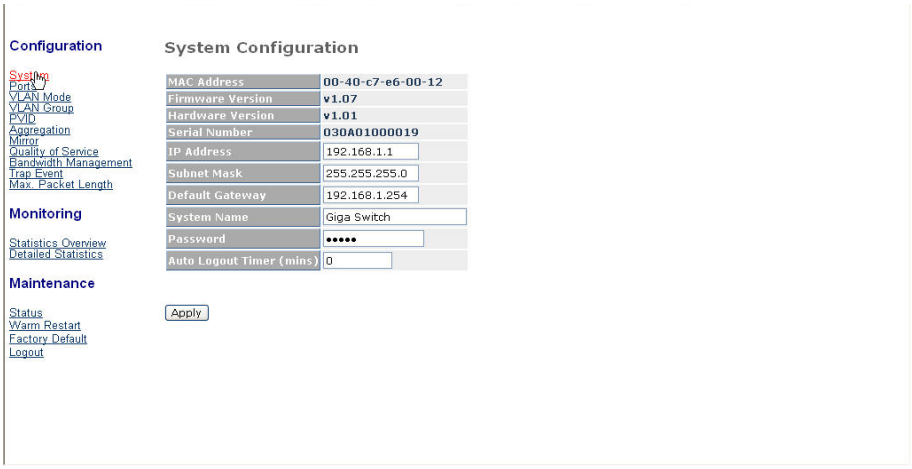


Fig. 4-3

Function name:

System Configuration

Function description:

Sets the IP address, subnet mask, default gateway, system name, password, and auto logout timer for the switch.

Parameter description:

MAC Address:

The Ethernet MAC address of the management agent in this switch.

Firmware Version:

The firmware version of this switch.

Hardware Version:

The hardware version of this switch.

Serial Number:

The serial number as assigned by Signamax.

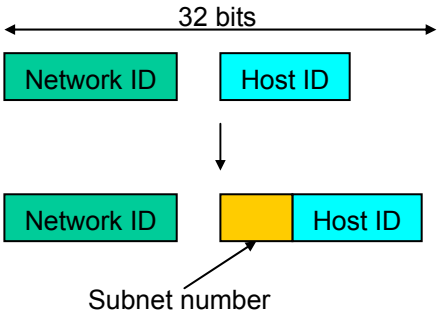
IP Address:

The user can configure the IP settings and fill in new values. When completed, click the **<Apply>** button to update.

Default: 192.168.1.1

Subnet Mask:

Subnet mask is made for the purpose of getting more network addresses, because any IP device in a network must own its IP address, composed of a Network address and a Host address, otherwise it can't communicate with other devices. Unfortunately, the network classes A, B, and C are all too large to fit for almost all networks; hence, a subnet mask is introduced to solve this problem. A Subnet mask uses some bits from the host address and makes an IP address look like a Network address, Subnet mask number and host address. This is shown in the following figure. This reduces the total number of IP addresses a network able to support, by the amount of the 2nd power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resident in the same network to which it is attached.

For more information, please also see the Section 2-1-4 "IP Address Assignment" in this manual.

Default: 255.255.255.0

Default Gateway:

Sets an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for another pre-defined path, it must be forwarded to a default router on a default path. This means any packet with an undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

System Name:

Sets a special user-defined name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and null are acceptable.

Default: Giga Switch

Password:

Sets a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.

Default: admin

Auto Logout Timer:

Sets the auto-logout timer. Valid values are 0 ~ 60 in units of minutes, and a decimal point is not allowed. The value 0 means the auto-logout timer is disabled.

Default: 0

4-2-2. Ports Configuration

Function name:

Ports Configuration

Function description:

Port Configuration is applied to change the setting of each port. By using this configuration capability, you can set/reset the Mode and Flow Control parameters. These functions are described in detail below.

Parameter description:

Mode:

Sets the speed and duplex mode of the port. If the media is 1 Gbps fiber, the speed is always 1000 Mbps and the only duplex mode permitted is full. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000 Mbps, and duplex mode, either full duplex or half duplex. The following table summarizes the functions the media supports.

Media type	NWay	Speed	Duplex
1000 M TP	ON/OFF	10/100/1000 M	Full for all, Half for 10/100
1000 M Fiber	ON/OFF	1000 M	Full

In Auto-negotiation mode, there is no default value. In Forced mode, default value depends on your settings.

Flow Control:

There are two modes to choose from in flow control, either Enable or Disable. If flow control is set to Enable, both parties can send a PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if the traffic is too much to handle.

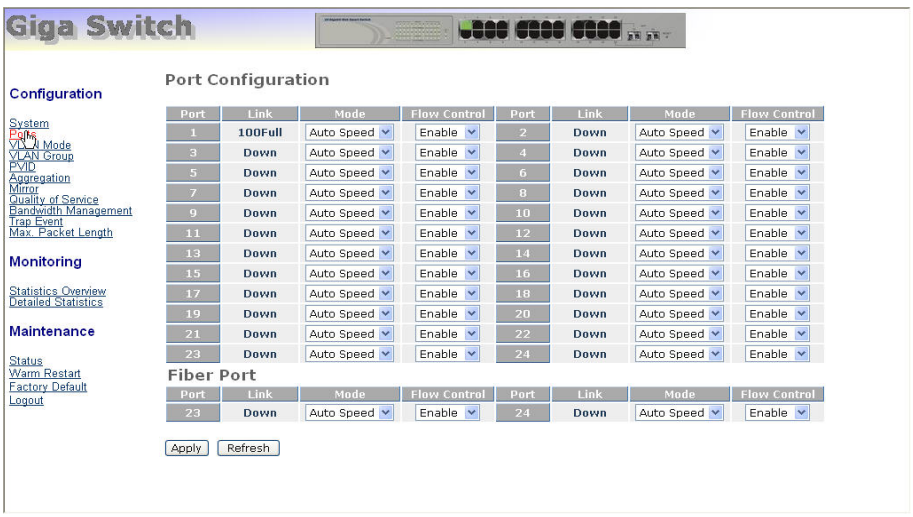

Giga Switch
Configuration
System
Port
VLAN Mode
VLAN Group
PVID
Aggregation
Mirror
Quality of Service
Bandwidth Management
Trap Event
Max. Packet Length
Monitoring
Statistics Overview
Detailed Statistics
Maintenance
Status
Warm Restart
Factory Default
Logout
Port Configuration
Port Link Mode Flow Control Port Link Mode Flow Control
1 100Full Auto Speed Enable 2 Down Auto Speed Enable
3 Down Auto Speed Enable 4 Down Auto Speed Enable
5 Down Auto Speed Enable 6 Down Auto Speed Enable
7 Down Auto Speed Enable 8 Down Auto Speed Enable
9 Down Auto Speed Enable 10 Down Auto Speed Enable
11 Down Auto Speed Enable 12 Down Auto Speed Enable
13 Down Auto Speed Enable 14 Down Auto Speed Enable
15 Down Auto Speed Enable 16 Down Auto Speed Enable
17 Down Auto Speed Enable 18 Down Auto Speed Enable
19 Down Auto Speed Enable 20 Down Auto Speed Enable
21 Down Auto Speed Enable 22 Down Auto Speed Enable
23 Down Auto Speed Enable 24 Down Auto Speed Enable
Fiber Port
Port Link Mode Flow Control Port Link Mode Flow Control
23 Down Auto Speed Enable 24 Down Auto Speed Enable
Apply
Refresh

Fig. 4-4

4-2-3. VLAN Mode Configuration

The switch supports Port-based VLAN and Tag-based VLAN (802.1q). It supports 24 active VLANs and VLAN IDs 1~4094. VLAN configuration is used to partition your LAN into small ones as your requirements demand. By properly configuring it, you can gain not only improved security and increased performance but you can also greatly reduce VLAN management time.

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes four modes: Port-based, Tag-based, Metro Mode, and Disable. The user can choose one of them by pulling down the list and pressing the **<Downward>** arrow key. Then, click the <**Apply>** button, and the settings will take effect immediately.

Parameter description:

VLAN Mode:

Disable:

Stops the VLAN function on the switch. In this mode, no VLAN is applied to the switch. This is the default setting.

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1, the VLAN contains member ports 1 & 2 & 3 & 4. If you are on port 1, you can communicate with ports 2 & 3 & 4. If you are on port 5, then you cannot communicate with them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to a maximum of 24 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports a supplement of 802.1Q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned a VLAN name and a VLAN ID. Valid VLAN IDs are 1-4094. User can create total of up to 24 Tagged VLAN groups.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method of Port-based VLAN. It will create 22 or 23 Port-based VLAN groups.

Fig. 4-5

Uplink Port:

This function is enabled only when metro mode is chosen as the VLAN mode.

23:

Except Port 23, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 23, thus, total 23 groups consisting of 2 members are formed.

24:

Except Port 24, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 24, thus, total 23 groups consisting of 2 members are formed.

23 & 24:

Except Port 23 and Port 24, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 23 and Port 24, thus, total 22 groups consisting of 3 members are formed.

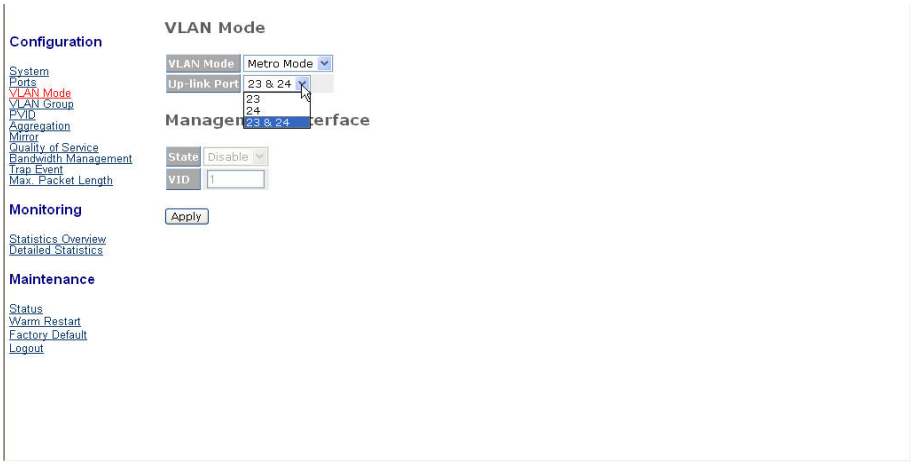


Fig. 4-6

Management Interface:

State:

Operates when the tag-based mode is chosen. When this function is enabled, only the tagged packets with this VID can manage the switch.

VID:

Valid range 1~4094.

4-2-4. VLAN Group Configuration

Function name:

VLAN Group Configuration

Function description:

This function shows the existing information of the VLAN Groups List and maintains them, i.e. modify and delete one of them. The user also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in a port-based VLAN, it will just show the ID、Description、Member of the existing port-based VLAN group. If you are in tag-based VLAN, it will show the ID、Description、VID、Member of the existing tag-based VLAN group. The switch cannot store the configuration of port-based VLANs and tag-based VLANs separately. When you choose one of the VLAN modes, the switch will bring you the responding VLAN configuration, which keeps the default data. The user can easily create and delete a VLAN group by pressing **<Add Group>** and **<Delete Group>** function buttons, or clicking the Group ID directly to edit it.

Parameter description:

ID (Group ID):

To edit a VLAN group, the user must select the Group ID field. Then, the user enters Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, depending on the desired VLAN mode selection.

Description:

The description defined by the administrator associated with a VLAN group.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

Used to enable or disable a port's membership in the newly-added VLAN, "Enable" establishes the port as a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

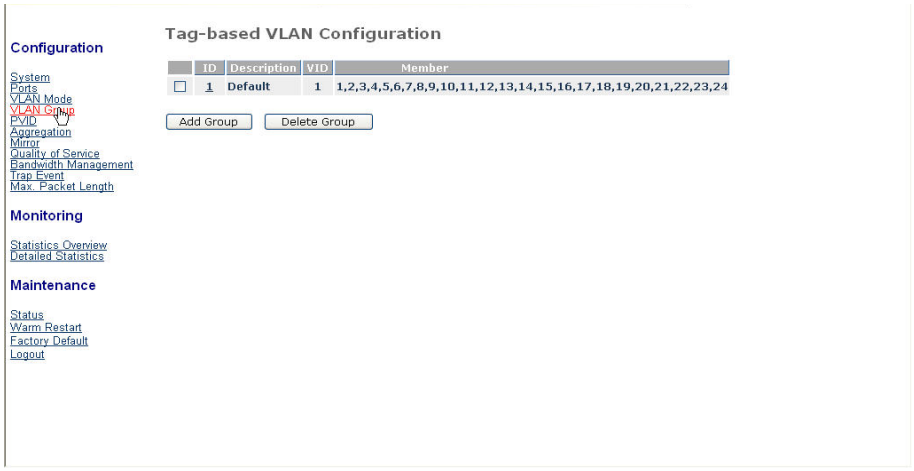


Fig. 4-7

Add Group:

Creates a new port-based VLAN or tag-based VLAN, depending on the VLAN mode the user selected in the VLAN mode function.

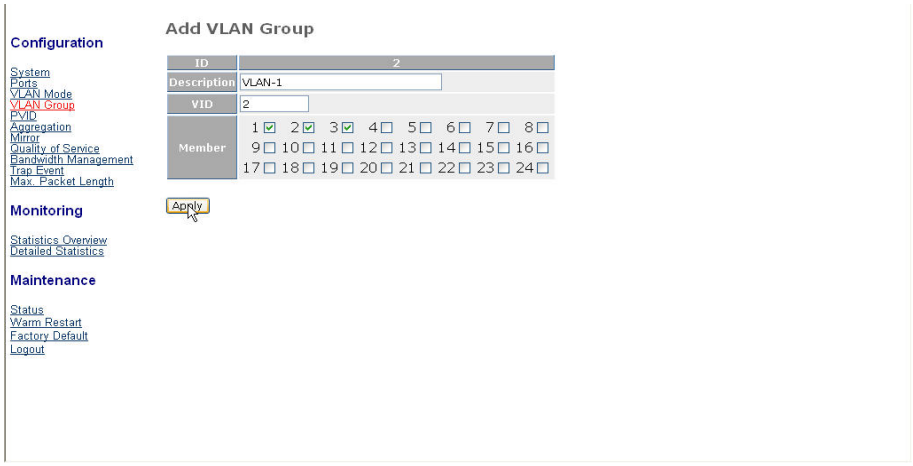


Fig. 4-8

Delete Group:

Just tick the check box (☑) beside the ID, then press the **<Delete Group>** button to delete the group.

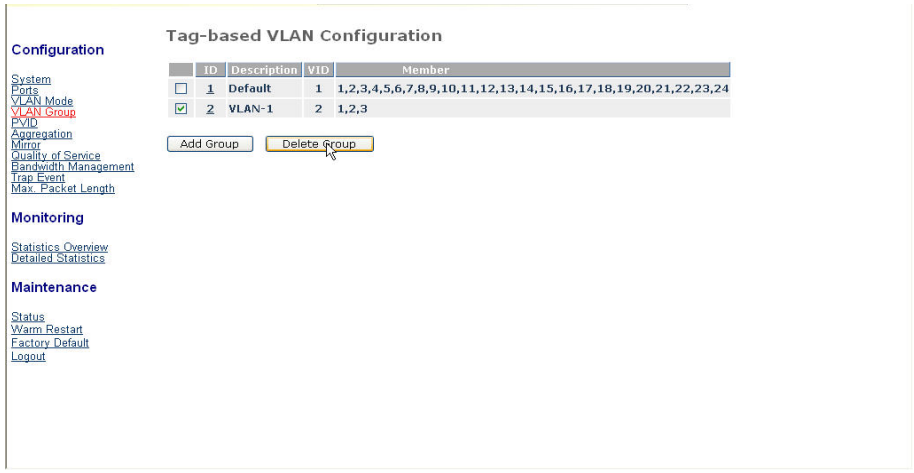


Fig. 4-9

4-2-5. PVID Configuration

Function name:

PVID Configuration

Function description:

In VLAN Port VID Setting, the user can input the VID number to each port. The range of valid VID numbers is from 1 to 4094. The user also can choose ingress filtering rules for each port. There are two ingress filtering rules which can be applied to the switch. Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. Ingress Filtering Rule 2 is “drop untagged frame”.

Parameter description:

Port 1-24:

Port number.

PVID:

The valid PVID range is 1-4094. Before a number x is set as a PVID, a Tag-based VLAN with VID x must be created. For example, if port x receives an untagged packet, the switch will apply the PVID (assumed in this example as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Rule 1:

Forward only packets with VID matching this port’s configured VID. Rule 1 can be applied as a way to use a given port to filter unwanted traffic. In Rule 1, a given port checks if the given port is a member of the VLAN on which the received packet belongs to, to determine whether to forward it or not. For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Rule 1 is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

Rule 2:

Drop untagged frame. The user can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frames. If the former is the case, then both tagged and untagged packets will be processed. If the latter is the case, only the packets carrying a VLAN tag will be processed, and the rest of the packets will be discarded.

Note: If Rule 1 is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, and the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

Tag:

This is an egress rule of the port. Valid rules are either “untag” or “tag”. Tag means the outgoing packets must carry a VLAN tag header; select this rule by ticking the check box (☑). Untag means the outgoing packets carry no VLAN tag header.

Untag State:

If the user has checked this function for a Tag out port, the packets from this port may be tag out. But the packet would be untag out if the VID of its tag is the same as the value of ”Untag VID” while the Untag VID state is Enable.

Untag VID:

Valid range is 0~4094.

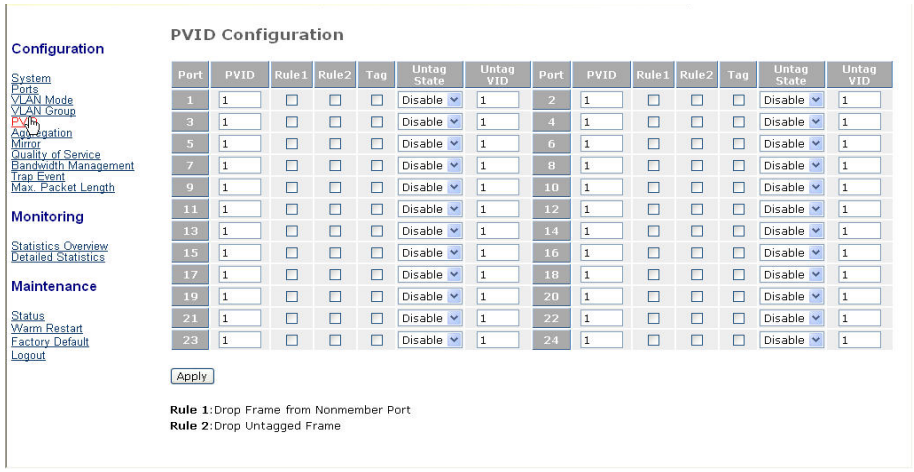

Configuration
System
Ports
VLAN Mode
VLAN Group
PVID
Aggregation
Mirror
Quality of Service
Bandwidth Management
Trap Event
Max. Packet Length
Monitoring
Statistics Overview
Detailed Statistics
Maintenance
Status
Warm Restart
Factory Default
Logout
PVID Configuration
Port PVID Rule1 Rule2 Tag Untag State Untag VID Port PVID Rule1 Rule2 Tag Untag State Untag VID
1 1 Disable 1 2 1 Disable 1
3 1 Disable 1 4 1 Disable 1
5 1 Disable 1 6 1 Disable 1
7 1 Disable 1 8 1 Disable 1
9 1 Disable 1 10 1 Disable 1
11 1 Disable 1 12 1 Disable 1
13 1 Disable 1 14 1 Disable 1
15 1 Disable 1 16 1 Disable 1
17 1 Disable 1 18 1 Disable 1
19 1 Disable 1 20 1 Disable 1
21 1 Disable 1 22 1 Disable 1
23 1 Disable 1 24 1 Disable 1
Apply
Rule 1:Drop Frame from Nonmember Port
Rule 2:Drop Untagged Frame

Fig. 4-10

4-2-6. Aggregation Configuration

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as that of a single Fast Ethernet port.

Function name:

Aggregation Configuration

Function description:

Displays the current setup of Aggregation Trunking. With this function, the user is allowed to add a new trunking group or modify the members of an existing trunking group.

Note:

Check the following to avoid errors in configuration:

When configuring the link aggregation function, the user should check that the aggregated ports are in full-duplex mode as well as whether their speed is the same or not. The aggregated ports are in the same VLAN group.

Parameter description:

Normal:

Set up the ports that do not join any aggregation trunking group.

Group 1~8:

Group the ports you choose together. Up to 12 ports can be selected for each group.

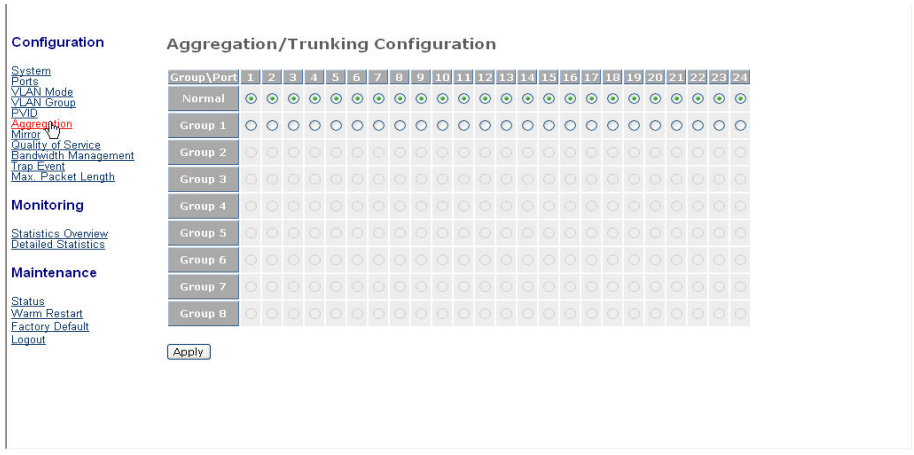


Fig. 4-11

4-2-7. Mirror Configuration

Function name:

Mirror Configuration

Function description:

Mirror Configuration is used to monitor the traffic of the network. For example, we assume that Port A and Port B are the Sniffer (Monitoring) Port and Source (Monitored) Port respectively; thus, the traffic received by Port B will be copied to Port A for monitoring.

Note:

When configuring the mirror function, the user should avoid setting a port to be a sniffer port and an aggregated port at the same time. It will cause data errors.

Parameter description:

Sniffer Mode:

Used for the activation or de-activation of Port Mirror function; the switch's port mirror function supports ingress traffic only. Default is "disable".

Sniffer Port:

Sets up the port for monitoring. Valid port is Port 1~24 and default is Port 1.

Source Port:

Sets up the port to be monitored. Just tick the check box (☑) under the port x; valid ports are Port 1~24.

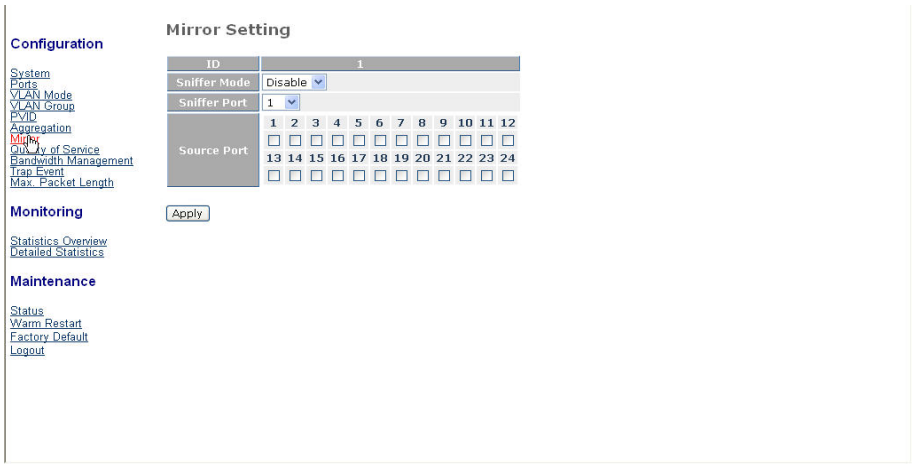


Fig. 4-12

4-2-8. Quality of Service Configuration

The switch offers powerful QoS functionality. This function supports VLAN-tagged priority that can assign precedence of up to 8 priorities; IP TOS Classification; IP TCP/UDP Port Classification; and IP DiffServ Classification.

In Quality of Service (QoS) Configuration, there is one option named ”Default Class”. If the user had selected one of the four QoS functions, then some packets that did not belong to this QoS setting would be viewed as Default Class. For instance, if you set the QoS function as VLAN Tag Priority mode, and then choose Default Class as High, then the priority of the packets with no tag will be considered as High priority precedence. The initial value of the Default Class is High.

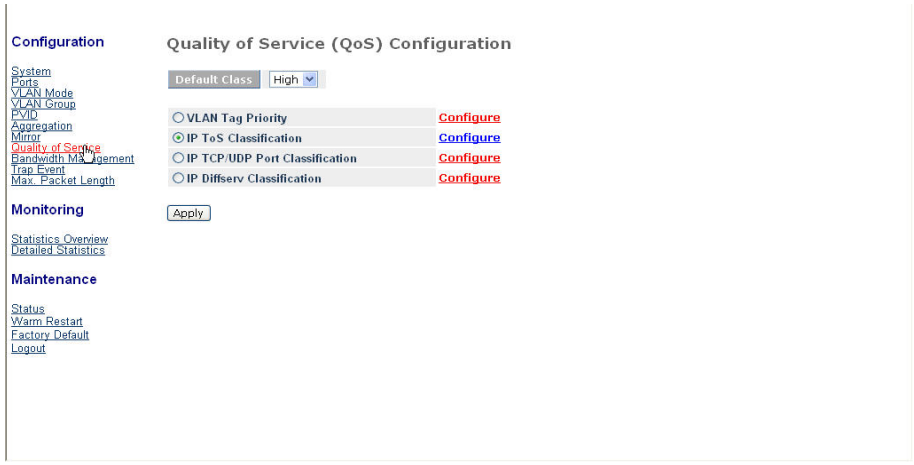


Fig. 4-13

Function name:

VLAN Tag Priority

Function description:

In VLAN tagging, there are 3 bits belonging to priority. According to these 3 bits, we could arrange 8 traffic classes –0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0, 1 1 1. We can set High priority or Low priority for each traffic class. For instance, let us let VLAN-tagged priority 0 0 0 be high priority and VLAN-tagged priority 0 0 1 be Low Priority, and then assign ports 1, 2, 3 to reside in VLAN 2. Packets are sent to ports 2 and 3 that have VLAN-tagged Field assigned as 0 0 0 and VID equals 2 from the port 2 and the packets that have VLAN-tagged Field appears 0 0 1 and VID equals 2 from the port 3. We let the two kinds of packets be transmitted to port 1 until the port results in congestion. The result is that the packets will be dropped partially from port 3, because the packets that emanate from there are assigned Low Priority. To use the VLAN Tag Priority function, please press the **<Configure>** button at the right section

In L4 QoS Configuration, you can enter a special network transmission event to prioritize it appropriately; for example we use ”Down prioritize web browsing, e-mail, FTP and news“ in the L4 QoS Configuration and click apply, and then click Custom L4. We can find Special TCP/UDP port 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have already existed and are defined for your use, but it is possible for you to modify this pre-defined TCP/UDP port with other port numbers you prefer. In ”Down prioritize web browsing, e-mail, FTP and news“, L4 QoS Configuration with a default setting, specially defined TCP/UDP port possesses a lower QoS traffic than Default class (all other TCP/UDP ports such as port 81,82,83,84,85,etc.). As an example, when we transmit TCP packets with port number 80 from port 2 and port number 81 from port 3 to port 1 until congestion occurs, the packets from port 3 will be dropped by port 1 because the TCP packets have port number 80 assigned as high priority and will have a higher precedence to be forwarded from port 1.

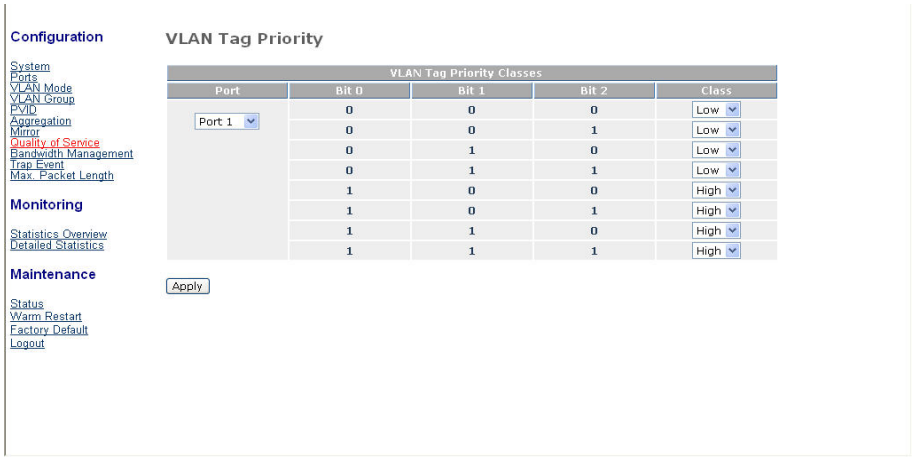


Fig. 4-14

Parameter description:

Quality of Service (QoS) VLAN Tag Configuration:

Used for setting up the QoS belonging to VLAN operation.

Port:

User can set up the port (1~24) respectively to let the VLAN Tag QoS function operate on them. If it is desirable to set up all ports at a time, the user is also allowed to choose “All” in the selection list to simplify the configuration procedure.

Bit 0, Bit 1, Bit 2:

According to the arrangement of VLAN-tagged priority, it can form 8 kinds of traffic classes, including 0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0
and 1 1 1.

Class:

8 kinds of traffic as mentioned above; the user can set up High Priority or Low Priority for each port respectively.

Function name:

IP TOS Classification

Function description:

Another QoS function is the application of Layer 3 on the network framework. This focuses on the TOS field of the IP header. There are three bits in the TOS field. Bits 2~4 of the TOS field are used. According to these 3 bits, 8 traffic classes can be arranged –0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0, 1 1 1. As long as bits 5~7 of the TOS field of the IP header are changed, we will create the 8 traffic packets intended. Moreover, High priority or Low priority can be set for each traffic class. For instance, if we let TOS 0 0 0 be high priority and TOS 0 0 1 be Low Priority, we sent in the packets that have bit 5~7 of TOS Field appear as 0 0 0 from port 2 and the packets that have bit 5~7 of TOS Field appear as 0 0 1 from port 3. We let the two kinds of packets be transmitted to port 1 until the port results in congestion. The result is that the packets will be dropped partially from port 3, because those packets are assigned Low Priority. To use the TOS Priority function, please press the **<Configure>** button at the right section to set it in advance.

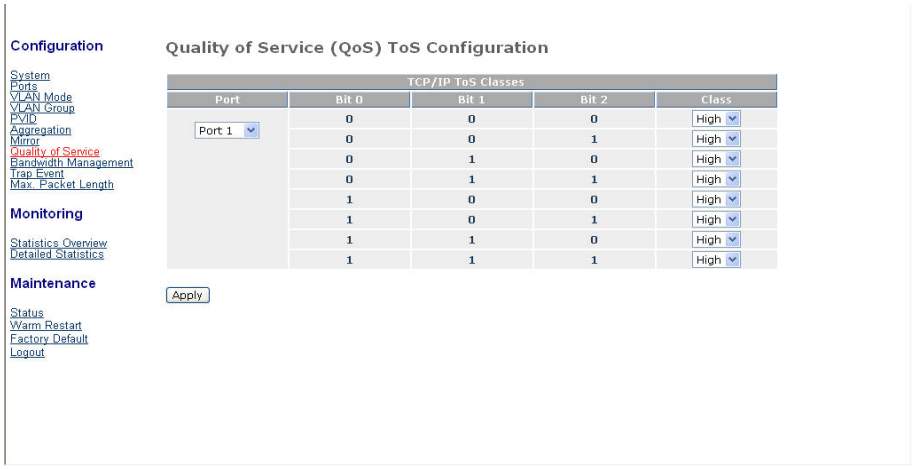


Fig. 4-15

Parameter description:

Quality of Service (QoS) ToS Configuration:

Used for setting up the QoS assignments in Layer 3.

Port:

The user can set up ports (1~24) respectively to let the TOS QoS function operate on them. If it is desirable to set up all ports at a time, the user is also allowed to choose “All” in the selection list to simplify the configuration procedure.

Bit 0, Bit 1, Bit 2:

According to the arrangement of Bit 5 ~ Bit 7 in TOS Field of IP Header, it can form 8 kinds of traffic classes, including 0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

8 kinds of traffic as mentioned above; the user can set up High Priority or Low Priority for each port respectively.

Function name:

IP TCP/UDP Port Classification

Function description:

In L4 QoS Configuration, you can enter a special network transmission event to prioritize it appropriately; for example we use ”Down prioritize web browsing, e-mail, FTP and news“ in the L4 QoS Configuration and click apply, and then click Custom L4. We can find Special TCP/UDP port 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have already existed and are defined for your use, but it is possible for you to modify this pre-defined TCP/UDP port with other port numbers you prefer. In ”Down prioritize web browsing, e-mail, FTP and news“, L4 QoS Configuration with a default setting, specially defined TCP/UDP port possesses a lower QoS traffic than Default class (all other TCP/UDP ports such as port 81,82,83,84,85,etc.). As an example, when we transmit TCP packets with port number 80 from port 2 and port number 81 from port 3 to port 1 until congestion occurs, the packets from port 3 will be dropped by port 1 because the TCP packets have port number 80 assigned as high priority and will have a higher precedence to be forwarded from port 1.

Parameter description:

Disable IP TCP/UDP Port Classification:

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to disable IP TCP/UDP port Classification for QoS.

Down prioritize web browsing, e-mail, FTP and news:

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize IP Telephony (VoIP):

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize iSCSI:

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize web browsing, e-mail, FTP transfers and news:

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize Streaming Audio/Video:

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):

Belongs to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Advanced Mode:

Displays the TCP/UDP port number in L4 QoS. In “Disable IP TCP/UDP Port Classification” mode, the user can randomly choose a TCP/UDP port number that L4 QoS will affect. As to other special L4 QoS events, a Special TCP/UDP port number will be taking action. The user could also be allowed to add or modify the port number at random. For instance, if we choose “Down prioritize web browsing, e-mail, FTP and news” as the QoS of L4 and enter the “Advanced Mode”, then we can see that some special port number 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have been configured already. The user also has the right to modify these port numbers. The display is shown in Fig 3-18.

Special TCP/UDP class:

There are two modes for selection, Low and High.

Default class (all other TCP/UDP ports):

There are two modes for selection, Low and High.

Port:

The user can set up the port (1~24) respectively to let Special TDP/UDP class functions operate on them. If it is desirable to set up all ports at a time, the user is also allowed to choose “All” in the selection list to simplify the configuration procedure.

Special UDP/TCP Port Selection:

The following are port numbers defined by six specific networks in L4:

- Down prioritize web browsing, e-mail, FTP and news: port number 80,280,443,25,110,20,21,69,119,2009
- Prioritize IP Telephony (VoIP):1718,1719,1720
- Prioritize iSCSI:3225,3260,3420
- Prioritize web browsing, e-mail, FTP transfers and news: 80,280,443,25,110,20,21,69,119,2009
- Prioritize Streaming Audio/Video: 2979,1755,7070,7071,554,8000
- Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):66,1571,1575,523,118,156,3306,1232,1433,1434

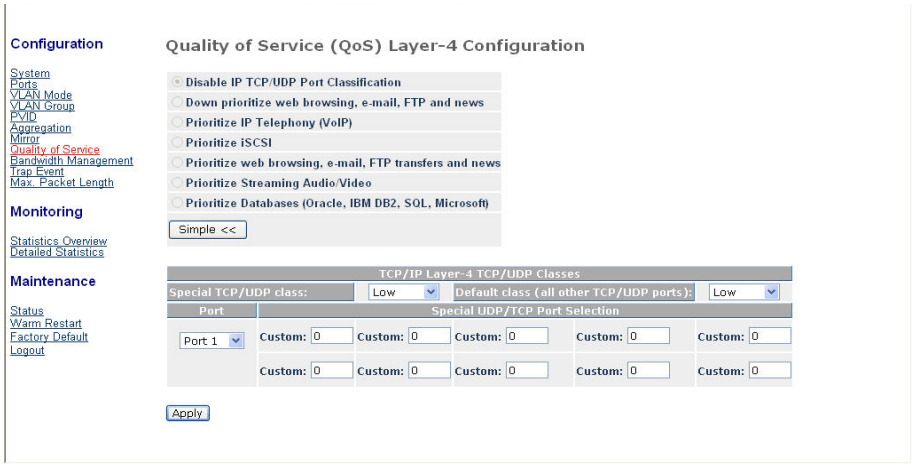


Fig. 4-16 Advanced Mode

Fig. 4-17 Simple Mode

Simple Mode:

Press **<Simple>** button is to return to the screen that all L4 port number will disappear (See Fig 4-17).

Function name:

IP DiffServ Classification

Function description:

Using the IP DiffServ Classification function, the switch can form a total of 64 (0~63) kinds of Traffic Class based on the arrangement of the 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to High or Low Priority.

Parameter description:

IP Differentiated Services (DiffServ) Configuration:

Used for setting up the IP Differentiated Services Configuration QoS.

DiffServ:

Display 64 (0~63) DiffServ Priority items.

Class:

64 kinds of traffic as described above; the user can set up High Priority or Low Priority for each port respectively.

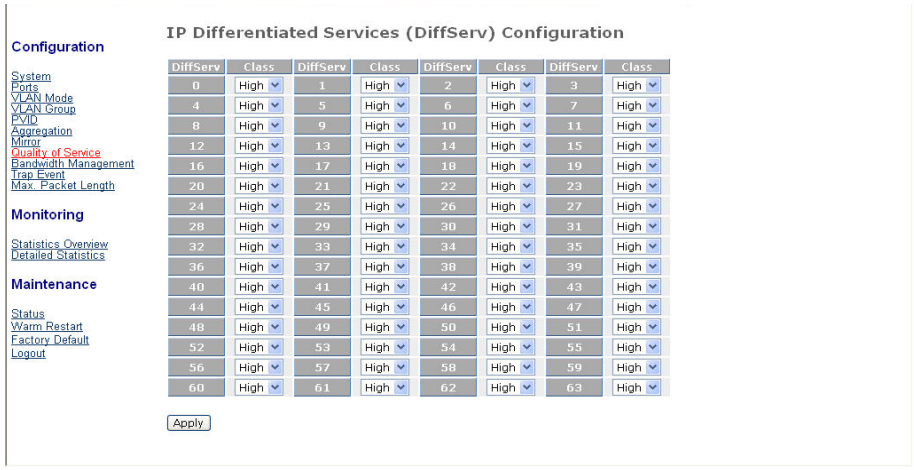

Configuration
System
Ports
VLAN Mode
VLAN Group
PVID
Aggregation
Mirror
Quality of Service
Bandwidth Management
Trap Event
Max. Packet Length
Monitoring
Statistics Overview
Detailed Statistics
Maintenance
Status
Warm Restart
Factory Default
Logout
IP Differentiated Services (DiffServ) Configuration
DiffServ Class DiffServ Class DiffServ Class DiffServ Class
0 High 1 High 2 High 3 High
4 High 5 High 6 High 7 High
8 High 9 High 10 High 11 High
12 High 13 High 14 High 15 High
16 High 17 High 18 High 19 High
20 High 21 High 22 High 23 High
24 High 25 High 26 High 27 High
28 High 29 High 30 High 31 High
32 High 33 High 34 High 35 High
36 High 37 High 38 High 39 High
40 High 41 High 42 High 43 High
44 High 45 High 46 High 47 High
48 High 49 High 50 High 51 High
52 High 53 High 54 High 55 High
56 High 57 High 58 High 59 High
60 High 61 High 62 High 63 High
Apply

Fig. 4-18

4-2-9. Bandwidth Management

Function name:

Bandwidth Management

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

Note:

Each port of the switch is assigned a 16 KB packet buffer. The packet buffer size will be reduced when the bandwidth rate limitation is enabled. This may cause jumbo frames not to be forwarded.

Please avoid enabling the jumbo frame capability and bandwidth rate limiting functions at the same time.

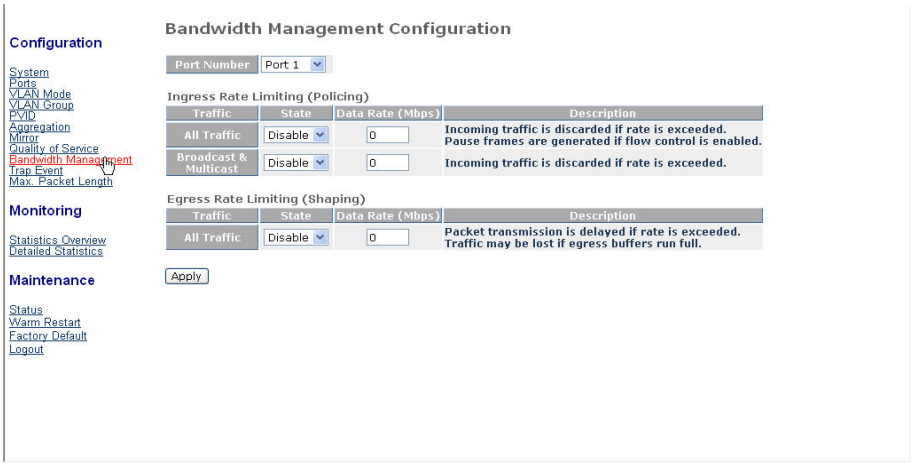


Fig. 4-19

Parameter description:

Port Number:

Choose the port on which you would like this function to operate. Valid range of the port is 1~24. The user is also permitted to choose “All” in the selection list to simplify the procedure of configuring. all ports at the same time

All Traffic for Ingress Rate Limiting:

Establishes the limit of Ingress bandwidth for the port selected. Incoming traffic will be discarded if the rate exceeds the value established in the Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

Broadcast & Multicast for Ingress Rate Limiting:

Establishes the limit of Ingress bandwidth for the port selected. Incoming traffic will be discarded if the rate exceeds the value established in the Data Rate field. The format of the packet limits this capability only to broadcast and multicast packets. Valid range is 0~1000.

All Traffic for Egress Rate Limiting:

Establishes the limit of Egress bandwidth for the port selected. Packet transmission will be delayed if the rate exceeds the value established in the Data Rate field. Traffic may be lost if egress buffers are filled. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

4-2-10. Trap Event Configuration

Function name:

Trap Event Configuration

Function description:

The Trap Events Configuration function is used to enable the Advanced Smart Ethernet Switch to send out the trap information while pre-defined trap events occurred.

Switch management offers 7 different trap events and 2 host to users .The message will be sent while users tick (☑) the trap event individually on the web page shown as below. Except Warm Boot and Cold Boot, other trap events offer the counter function to help the user see the times that the trap event had happened.

Parameter description:

These trap functions are as they describe. The traps the switch supports are listed below.

Boot: Warm Boot, Cold Boot

Login: Illegal Login

Link: Link Up, Link Down

Tx/Rx error: Rx error threshold, Tx error threshold

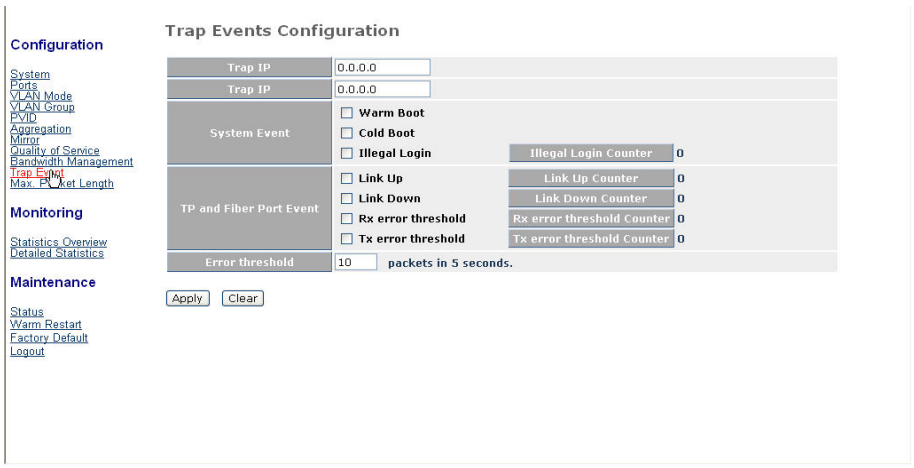


Fig. 4-20

4-2-11. Max. Packet Length

Function name:

Max. Packet Length

Function description:

The switch is capable of dealing with 9k Jumbo Frames, which suits the transmission for a large amount of data in the network environment.

Parameter description:

Jumbo Frame (bytes):

Set up the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1532 bytes.

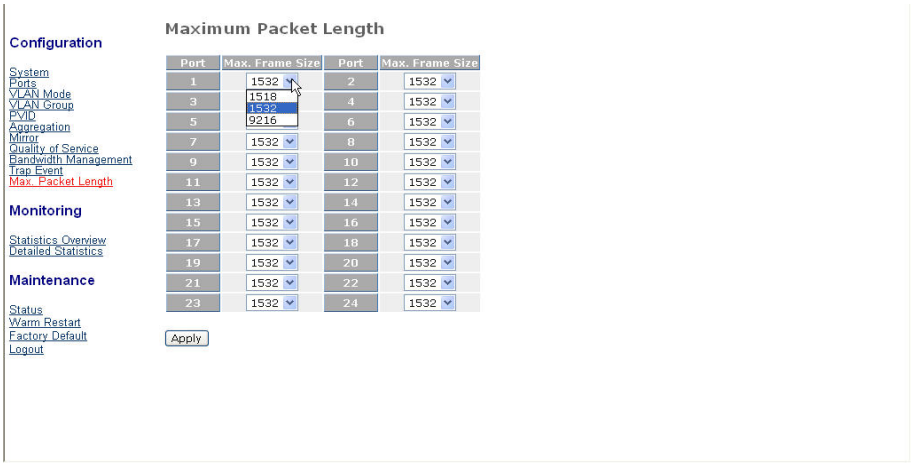
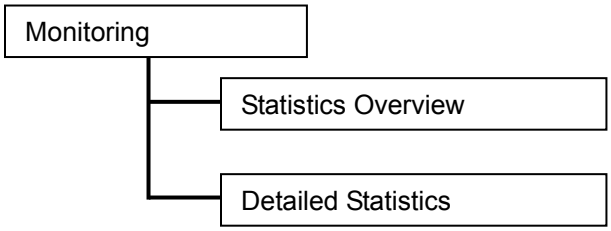


Fig. 4-21

4-3. Monitoring

There are two functions contained in the monitoring section.



4-3-1. Statistics Overview

The function of Statistics Overview collects any information and provides the counting summary about the traffic of the port, no matter the packet is good or bad.

In the Fig. 4-22, the window can show all ports' counter information at the same time. If the counting is overflow, the counter will be reset and restart counting.

Function name:

Statistics Overview

Function description:

Display the summary counting of each port's traffic, including Tx Bytes, Tx Frames, Rx Bytes, Rx Frames, Tx Errors and Rx Errors.

Parameters description:

Tx Byte:

Total transmitted bytes.

Rx Byte:

Total received bytes.

Tx Packet:

The counted number of packets transmitted.

Rx Packet:

The counted number of packets received.

Tx Collision:

Number of collisions transmitting frames experienced.

Rx Error Packet:

Number of bad packets received.

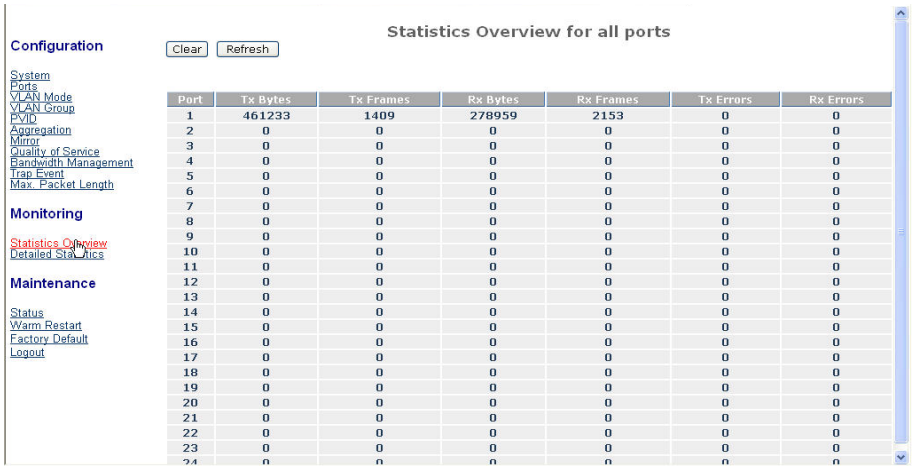

Configuration
System
Ports
VLAN Mode
VLAN Group
PVID
Aggregation
Mirror
Quality of Service
Bandwidth Management
Trap Event
Max. Packet Length
Monitoring
Statistics Overview
Detailed Statistics
Maintenance
Status
Warm Restart
Factory Default
Logout
Statistics Overview for all ports
Clear
Refresh
Port Tx Bytes Tx Frames Rx Bytes Rx Frames Tx Errors Rx Errors
1 461233 1409 278959 2153 0 0
2 0 0 0 0 0 0
3 0 0 0 0 0 0
4 0 0 0 0 0 0
5 0 0 0 0 0 0
6 0 0 0 0 0 0
7 0 0 0 0 0 0
8 0 0 0 0 0 0
9 0 0 0 0 0 0
10 0 0 0 0 0 0
11 0 0 0 0 0 0
12 0 0 0 0 0 0
13 0 0 0 0 0 0
14 0 0 0 0 0 0
15 0 0 0 0 0 0
16 0 0 0 0 0 0
17 0 0 0 0 0 0
18 0 0 0 0 0 0
19 0 0 0 0 0 0
20 0 0 0 0 0 0
21 0 0 0 0 0 0
22 0 0 0 0 0 0
23 0 0 0 0 0 0

Fig. 4-22

4-3-2. Detailed Statistics

Function name:

Detailed Statistics

Function description:

Displays the detailed count number of each port's traffic. As shown in Fig. 4-23, the window can show all counter information of each port at one time.

Parameter description:

Rx Packets:

The counted number of packets received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

The counted number of broadcast packets received.

Rx Multicast:

The counted number of multicast packets received.

Tx Packets:

The counted number of packets transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

The counted number of broadcast packets transmitted.

Tx Multicast:

The counted number of multicast packets transmitted.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames (according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames (according to max_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receive buffer space.

Rx Errors:

Number of errored packets received.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops:

Number of frames dropped due to the lack of transmit buffer space.

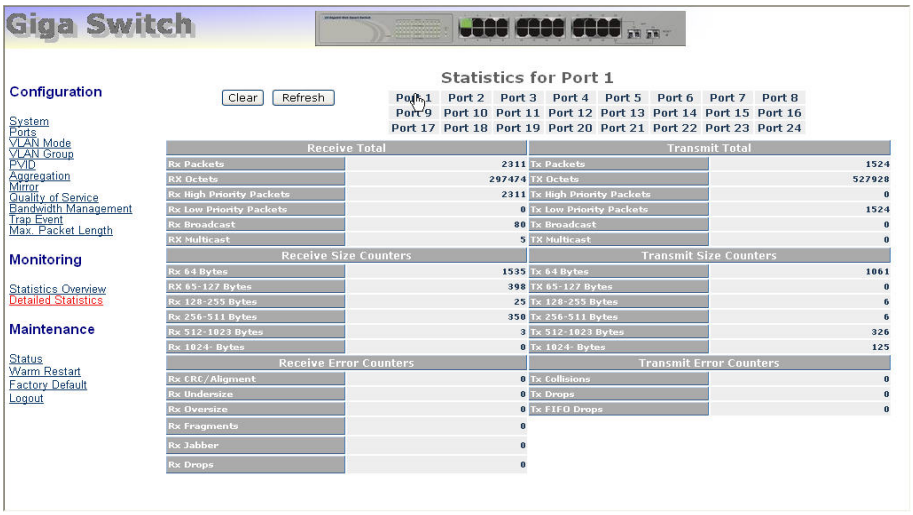
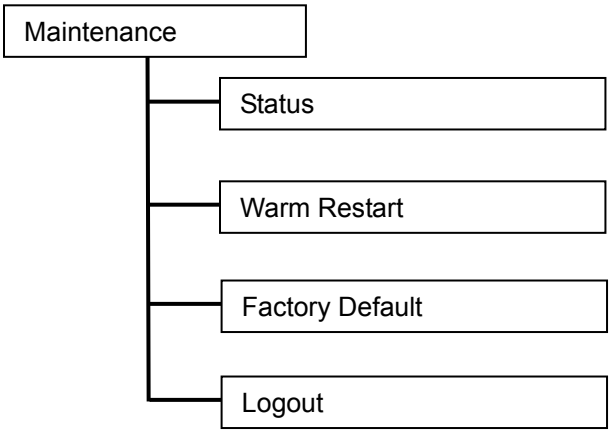


Fig. 4-23

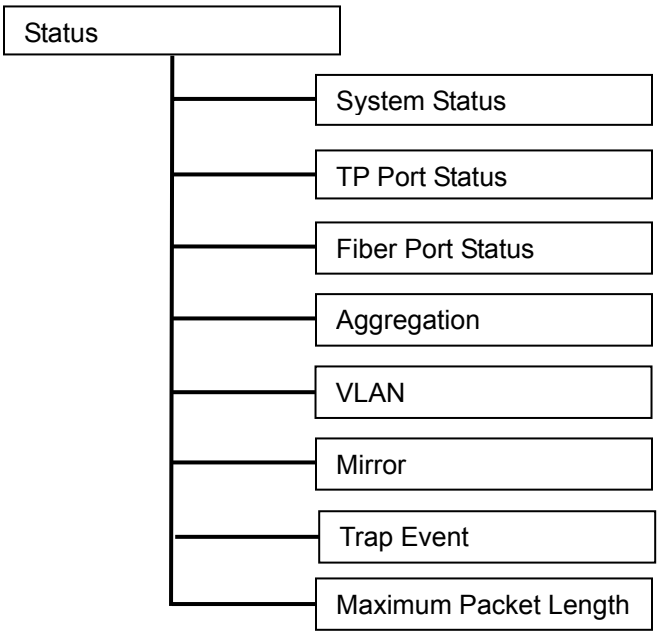
4-4. Maintenance

There are four functions contained in the maintenance section.



4-4-1. Status

Eight functions, including System Status, TP Port Status, Fiber Port Status, Aggregation, VLAN, Mirror, Trap Event and Maximum Packet Length are contained in this function folder for port monitoring and management. Each of them will be described in detail in the following sections.



4-4-1-1.System Status

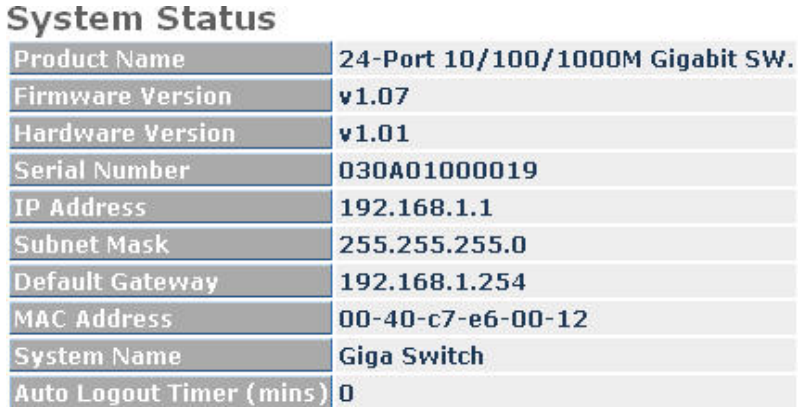


Fig. 4-24

Function name:

System Status

Function Description:

Displays the status information of this switch.

Parameter Description:

Product Name:

Displays the product name of this device.

Firmware Version:

Displays the firmware version of this switch.

Hardware Version:

Displays the hardware version of this switch.

Serial Number:

Displays the serial number as assigned by Signamax.

IP Address:

Displays the IP address of this switch.

Subnet Mask:

Displays the subnet mask of this switch.

Default Gateway:

Displays the default gateway of this switch.

MAC Address:

Displays the Ethernet MAC address of this switch.

System Name:

Displays the name of the switch. User-defined.

Auto Logout Timer:

Displays the setting of auto-logout timer in the web UI.

4-4-1-2. TP / Fiber Ports Status

Function name:

TP/Fiber Ports Status

Function description:

Reports the latest updated status of all ports in this switch. Using this function, the user can view the following settings: link status, speed and flow control. All settings are described in detail below.

TP Port Status

Port	Link Status	Speed	Flow Control	Port	Link Status	Speed	Flow Control
1	100FDX	Auto	Enabled	2	Down	Auto	Enabled
3	Down	Auto	Enabled	4	Down	Auto	Enabled
5	Down	Auto	Enabled	6	Down	Auto	Enabled
7	Down	Auto	Enabled	8	Down	Auto	Enabled
9	Down	Auto	Enabled	10	Down	Auto	Enabled
11	Down	Auto	Enabled	12	Down	Auto	Enabled
13	Down	Auto	Enabled	14	Down	Auto	Enabled
15	Down	Auto	Enabled	16	Down	Auto	Enabled
17	Down	Auto	Enabled	18	Down	Auto	Enabled
19	Down	Auto	Enabled	20	Down	Auto	Enabled
21	Down	Auto	Enabled	22	Down	Auto	Enabled
23	Down	Auto	Enabled	24	Down	Auto	Enabled

Fiber Port Status

23	Down	Auto	Enabled	24	Down	Auto	Enabled

Fig. 4-25

Parameter description:

Port:

Displays the port number. The number is 1 – 24. Both port 23 and 24 are optional modules.

Link Status:

Indicates if the link on the port is active or not. If the link is connected to a properly-working device, the Link status will show the link “Up”; otherwise, it will show “Down”. This is determined by the hardware devices on both ends of the connection.

No default value.

Speed:

Displays the speed and duplex mode of all ports. There are three speeds (10 Mbps, 100 Mbps and 1000 Mbps) supported for TP media, and the duplex modes supported are half duplex and full duplex. If the media is 1 Gbps fiber, the 1000 Mbps speed is the only one supported. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in “Auto Speed” mode or 2) user setting in “Force” mode. The local port has to have its capability preset

Flow Control:

Shows each port's flow control status.

There are two types of flow control in Ethernet: Backpressure for half-duplex operation, and Pause flow control (IEEE 802.3x) for full-duplex operation. The switch supports both of these types of flow control.

Default: Enabled

4-4-1-3. Aggregation

Function name:

Aggregation Status

Function description:

Displays the current setup of Aggregation Trunking.

Parameter description:

Normal:

Displays the ports that are not a member of any aggregation trunking group.

Group 1~8:

Displays the members of the Group.

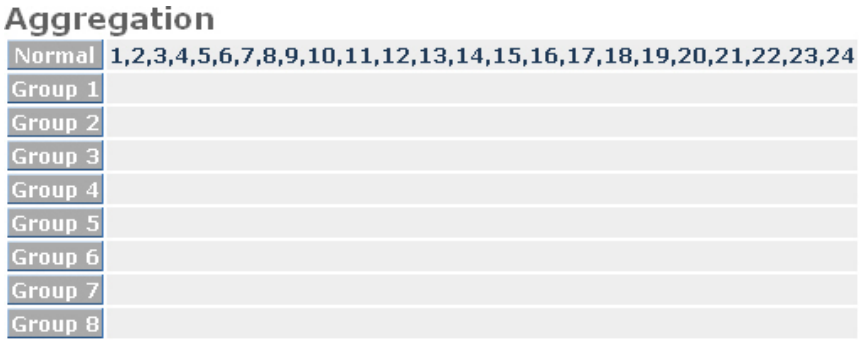


Fig. 4-26

4-4-1-4. VLAN

Function name:

VLAN Status

Function description:

Display the status of the VLAN mode and VLAN group settings.

Parameter description:

VLAN Mode:

Displays Port-based, Tag-based and metro mode, depending on the setting established in the VLAN mode configuration function.

ID:

Displays the Group ID.

Description:

Displays the description defined by the administrator that is associated with a VLAN group.

VID:

Displays the VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in the Tag-based mode.

Member:

Displays the member ports belonging to each VLAN Group.

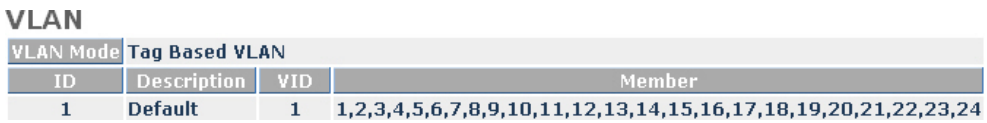


Fig. 4-27 Tag-based VLAN

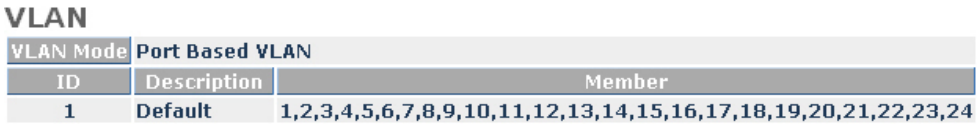
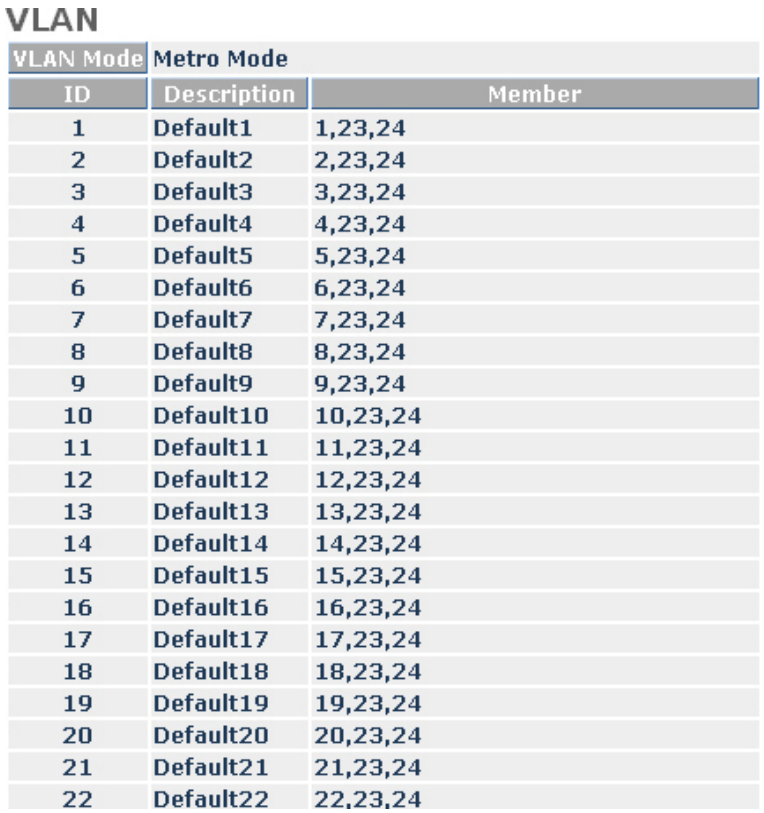


Fig. 4-28 Port-based VLAN



VLAN

VLAN Mode: Metro Mode

ID	Description	Member
1	Default1	1,23,24
2	Default2	2,23,24
3	Default3	3,23,24
4	Default4	4,23,24
5	Default5	5,23,24
6	Default6	6,23,24
7	Default7	7,23,24
8	Default8	8,23,24
9	Default9	9,23,24
10	Default10	10,23,24
11	Default11	11,23,24
12	Default12	12,23,24
13	Default13	13,23,24
14	Default14	14,23,24
15	Default15	15,23,24
16	Default16	16,23,24
17	Default17	17,23,24
18	Default18	18,23,24
19	Default19	19,23,24
20	Default20	20,23,24
21	Default21	21,23,24
22	Default22	22,23,24

Fig. 4-29 Metro mode VLAN

4-4-1-5. Mirror

Function name:

Mirror Status

Function description:

Mirror Status is used to display the results of the mirror configuration setting.

Parameter description:

Sniffer Mode:

Displays the activation or de-activation status of the Port Mirror function. Default is "Disable".

Sniffer Port:

Displays the port used for monitoring. Valid port range is Port 1~ 24; default is Port 1.

Source Port:

Display the port for being monitored. Valid port range is Port 1~ 24.

Fig. 4-30

4-4-1-6. Trap Event

Function name:

Trap Event Status

Function description:

The Trap Events status function is used to display the switch's trap information sent out when pre-defined trap events occur.

Parameter description:

The names of the trap functions are self-descriptive. The traps that the switch supports are listed below.

Boot: Warm Boot, Cold Boot

Login: Illegal Login

Link: Link Up, Link Down

Tx/Rx error: Rx error threshold, Tx error threshold

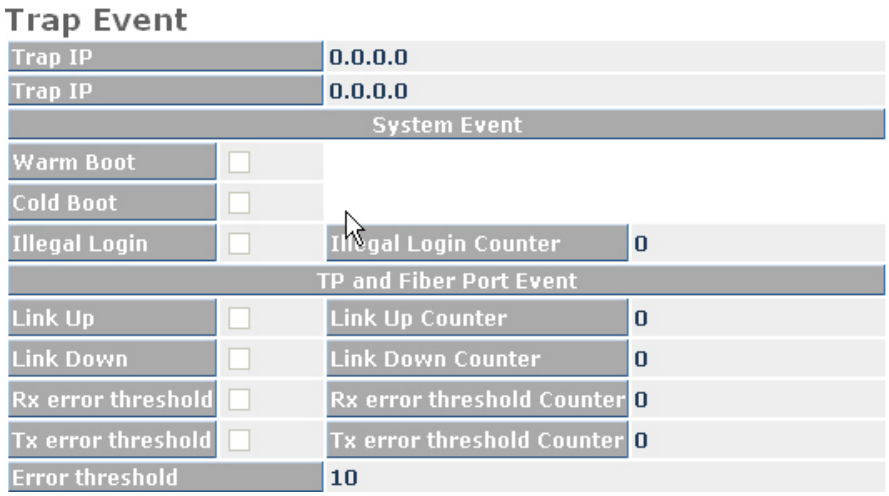


Fig. 4-31

4-4-1-7. Maximum Packet Length

Function name:

Max. Packet Length Status

Function description:

Displays the maximum packet length settings that each port can accept in this switch.

Parameter description:

Jumbo Frame (bytes):

Displays the settings that determine the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1532 bytes.

Maximum Packet Length

Port	Max. Frame Size	Port	Max. Frame Size
1	1532	2	1532
3	1532	4	1532
5	1532	6	1532
7	1532	8	1532
9	1532	10	1532
11	1532	12	1532
13	1532	14	1532
15	1532	16	1532
17	1532	18	1532
19	1532	20	1532
21	1532	22	1532
23	1532	24	1532

Fig. 4-32

4-4-2. Warm Restart

The user has many ways to reboot the switch, including power up, hardware reset and software reset. Pressing the RESET button in the front panel resets the switch. After upgrading software, the switch must be rebooted to have the new configuration take effect. The function discussed here provides a software reset for the “reboot” in the main menu.

Function name:

Warm Restart

Function description:

Reboots the switch. Reboot has the same effect as the RESET button on the front panel of the switch. After pressing the **<Yes>** button to confirm the warm restart function, it will take approximately thirty (30) seconds to complete the system boot.

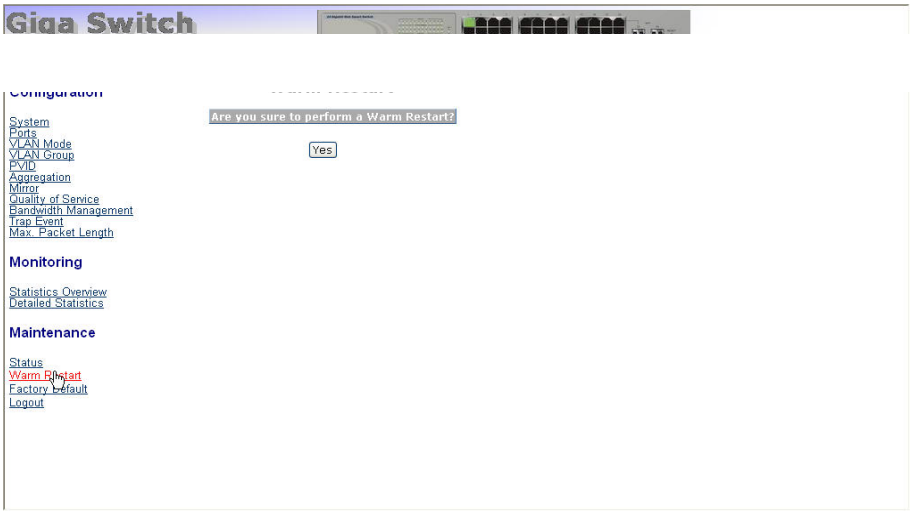


Fig. 4-33

4-4-3. Factory Default

Function name:

Factory Default

Function description:

The Factory Default Configuration function can retrieve the switch's default setting to replace the working configuration. Except for the IP address setting, all configurations will be restored to the factory default value when the user runs the "Factory Default" function in the web UI. If the user prefers to restore all configurations ***including*** the IP address setting to the factory default, press the "RESET" button on the front panel.

Note \the "RESET" button must be pressed for longer than 3 seconds to restore the factory default setting.

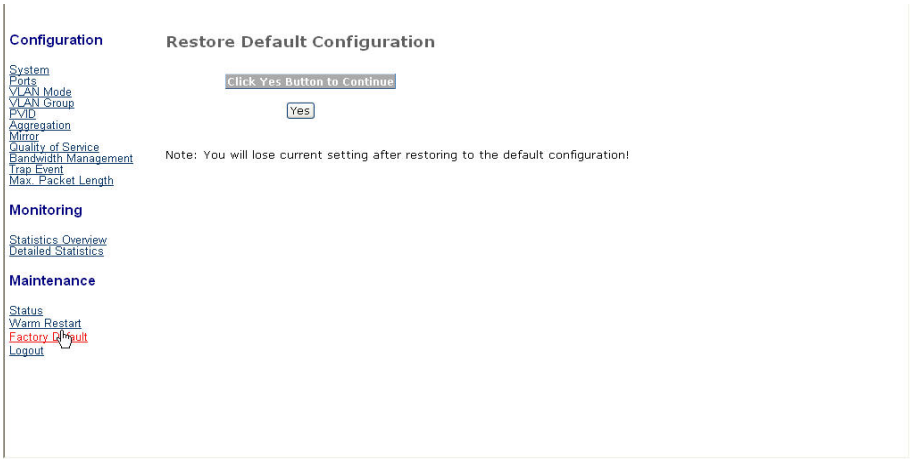


Fig. 4-34

4-4-4. Logout

The user can manually logout of the switch management software by performing the Logout function. The switch also provides an automatic logout capability, which is user-configured.

Function name:

Logout

Function description:

The switch allows the user to log out of the system to prevent other users from using the system without permission. If the user does not logout and exits the browser, the switch will automatically log the user out. Besides this manual logout and implicit logout, the user can set up the Auto Logout Timer parameter in the system configuration function to explicitly turn this logout function ON or OFF..

Parameter description:

Auto/Manual Logout:

Default is ON. If it is “ON”, and no action is taken and no keystroke has occurred as well in any function screen for more than the number of minutes programmed in the Auto Logout Timer, the switch will log the user out automatically The user can also press the **<Logout>** button to exit the system manually.

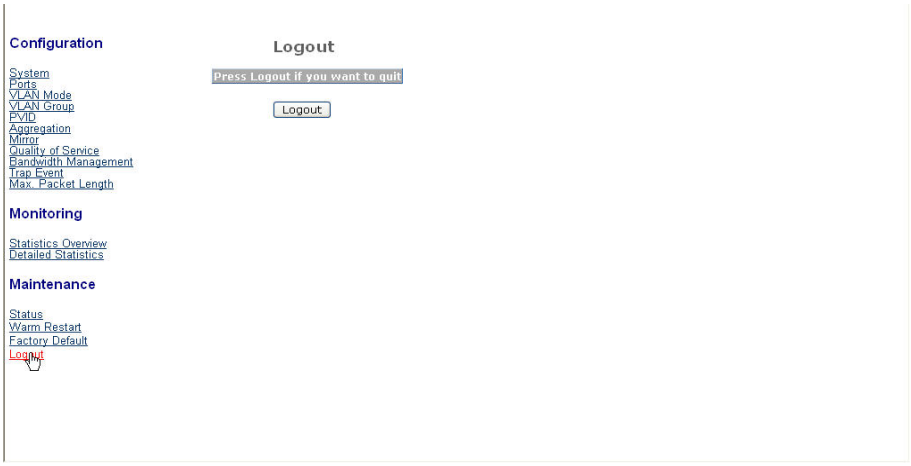


Fig. 4-35

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.
   - ✓ The network interface of Computer C may have failed. Please check the link/activity status of Computer C on the LED indicator of Computer C's network interface as well as that of the switch. Try another network device on this connection.
   - ✓ The network configuration of Computer C may be incorrect. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.
   - ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that Switch.
   - ✓ Please check the uplink setup of the Switch to verify that the uplink function is enabled.

3. The console interface cannot appear on the console port connection.
   - ✓ The 065-7941 WebSmart Switch has no console port, so you cannot use a local console interface to connect with this Switch.

4. How is the 065-7941 Gigabit WebSmart Switch configured?
   - ✓ The user can use the IE browser program in Microsoft Windows-equipped computers or another web browser program to control the WebSmart functions in the 065-7941 Gigabit WebSmart Switch. First, connect to any port of the 065-7941 Switch. Then, using the web browser, type the default IP address, 192.168.1.1, to connect to the 065-7941 with an Ethernet network connection. The login screen will appear at once.

Appendix A
Technical Specifications

Features

- 22 (10/100/1000 Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE 802.3, 802.3u, 802.3z and 802.3ab.
- 2 Gigabit TP/SFP fiber ports are dual media ports with an auto-detection function.
- Non-blocking store-and-forward shared-memory, Web-Smart switched.
- Supports auto-negotiation for configuring speed and duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any of the ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Web-based management provides the ability to completely manage the switch from any web browser.
- Supports Port-based VLAN and Protocol-based (IEEE 802.1Q) VLAN.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Prioritization of Service (a.k.a. Class of Service) with 2-level priority queuing.
- Supports port trunking with flexible load distribution and failover function.
- Supports port sniffer functionality via the Port Mirroring feature
- Programmable maximum Ethernet frame length ranging from 1518 to 9216 bytes jumbo frame.
- Efficient self-learning and address recognition mechanism enables wire speed forwarding rates.

Hardware Specifications

- **Standard Compliance:**
  IEEE 802.3 10BaseT
  IEEE 802.3u 100BaseTX
  IEEE 802.3ab 1000BaseT
  IEEE 802.3z 1000BaseSX/LX
  IEEE 802.1p Priority (Quality of Service [QoS])
  IEEE 802.1Q Tagged VLAN
  IEEE 802.3x Flow Control

- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000 Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 24
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	23,24(Optional)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	23,24(Optional)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	23,24(Optional)

*Port 23, 24 are TP/SFP fiber dual media ports with auto-detection function
*Optional SFP module supports LC or BiDi LC transceiver

- **Transmission Mode:** 10/100 Mbps supports full or half duplex
  1000 Mbps supports full duplex only

- **Transmission Speed:** 10/100/1000 Mbps for TP
  1000 Mbps for Fiber

- **Full Forwarding/Filtering Packet Rate:**

Forwarding Rate	Speed
1,488,000 pps	1000 Mbps
148,800 pps	100 Mbps
14,880 pps	10 Mbps

(pps = packets per second)

- **MAC Address and Self-learning:** 8K MAC addresses
  4K VLAN table entries

- **Buffer Memory:** Embedded 400 KB frame buffer

- **Flow Control:** IEEE 802.3x compliant for full duplex
  Backpressure flow control for half duplex

- **Cable Type and Maximum Length:**

TP	Cat. 5e or better UTP cable, up to 100 m
1000BaseSX	Up to 220/275/500/550 M, which depends on Multimode Fiber type
1000BaseLX	Single-Mode Fiber, up to10/30/50 km
1000BaseLX WDM (BiDi)	Single-Mode Single Fiber, up to 20 km

- **Diagnostic LEDs:**
  System LEDs : Power, CPU
  Per Port LEDs:
  10/100/1000 Mbps TP Ports 1 to 24: LINK/ACT, 10/100/1000 Mbps
  1000 Mbps SFP Fiber Ports 23 & 24: SFP (LINK/ACT)

- **Power Requirement:**
  Voltage: 100~240 Volts AC
  Frequency: 50~60 Hz
  Power Consumption: 30 Watts

- **Ambient Temperature:** 32° to 122°F [0° to 50°C]
- **Humidity:** 5% to 90%
- **Dimensions:** 1.73 in.(H) × 17.4 in.(W) × 8.23 in.(D) [44 × 442 × 209 mm]
- **Emissions:** Complies with FCC Part 15, Class A & CE Mark Approval

Management Software Specifications

System Configuration	Auto-negotiation support on 10/100/1000 Base-TX ports, Web browser or console interface can set transmission speed (10/100/1000 Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
VLAN Function	Port-Base / 802.1Q-Tagged, allowed up to 256 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
Bandwidth Control	Supports by-port Egress/Ingress rate control
Quality of Service (QoS)	Referred as Class of Service (CoS) by the IEEE 802.1P standard Two queues per port
Network Management	Web browser support based on HTTP Server

Note: Any specification is subject to change without notice.